面向21世纪课程教材
Textbook Series for 21st Century

近世代数基础

刘绍学

高等教育出版社
HIGHER EDUCATION PRESS

VISIT…

LANZAROTE Caliente.com

面 向 2 1 世 纪 课 程 教 材
Textbook Series for 21st Century

近世代数基础

刘绍学

高等教育出版社
HIGHER EDUCATION PRESS

(京)112 号

内容提要

本书是教育部“高等教育面向21世纪教学内容和课程体系改革计划”的研究成果，是面向21世纪课程教材和普通高等教育“九五”国家级重点教材。本书作者在介绍近世代数课程的传统内容时，在以下各方面进行了有益的探索：强调代数系统的出现是刻画物理量和几何量的需要；较深入地介绍一些具体的群、环、域以及介绍代数的应用；注意讲授近世代数中的数学思想等。全书共四章及一个附录。第一章由刻画“对称”而引入群的概念；第二章介绍群论基础；第三章介绍环、域和模；第四章介绍有限域和 Galois 理论；附录介绍了计算代数几何的基石——Gröbner 基和 Buchberger 算法。

本书可作为高等学校数学专业的教科书，也可供相关专业师生和有关科研人员参考。

图书在版编目(CIP)数据

近世代数基础/刘绍学. －北京：高等教育出版社，
1999
面向21世纪教材 普通高等教育“九五”国家级重点教
材
ISBN 7－04－007450－8

Ⅰ.近… Ⅱ.刘… Ⅲ.抽象代数－高等教育－教材 Ⅳ.0
153

中国版本图书馆 CIP 数据核字(1999)第64453号

近世代数基础
刘绍学

出版发行	高等教育出版社		
社　址	北京市东城区沙滩后街55号	邮政编码	100009
电　话	010－64054588	传　真	010－64014048
网　址	http://www.hep.edu.cn		
经　销	新华书店北京发行所		
印　刷	国防工业出版社印刷厂		
纸张供应	山东高唐纸业集团总公司		
开　本	787×960　1/16	版　次	1999年10月第1版
印　张	13.5	印　次	1999年10月第1次印刷
字　数	200 000	定　价	14.60元

凡购买高等教育出版社图书，如有缺页、倒页、脱页等
质量问题，请在所购图书销售部门联系调换。

版权所有　侵权必究

序　言

代数学是以数、多项式、矩阵、变换和它们的运算，以及群、环、域和模等为研究对象的学科. 简单地说，代数学是研究代数系统（带有一些运算的集合）的. 我们知道，数、多项式和矩阵的出现是由于刻画现实世界中几何量和物理量的需要. 同样，群等也是由于直接或间接刻画新的几何量和物理量的需要而出现的. 这样，研究这些对象就有两种途径：第一种是紧密结合它们出现的背景去研究，例如用群论方法去研究晶体的分类等；第二种是把数、多项式、矩阵、群等作为数学对象去研究，这时常和它们出现的背景相去甚远，或者几乎完全脱离这些背景. 然而这两种研究应该是相辅相成浑然一体的.

在编写本书时，我们有以下的一些考虑.

一、在本课程中我们试图进行一些探索，在内容上除了第二、三、四章给出本课程的传统内容外，我们安排了第一章的“对称与群”和附录的“多元多项式环”. “对称与群”强调抽象代数系统的出现是由于刻画物理量和几何量的需要. “多元多项式环”中主要介绍 Gröbner 基，Buchberger 算法，它们是计算代数几何的基石，同时又是“初等”的，其难度和深度适中，是能够放在基础课中的. 这使我们有一个恰当的方式来介绍多元多项式环这个重要的具体环，并能突出算法这个有用的数学概念以及代数与计算机的联系. 虽然讲此内容可能有时间上的困难，但为了保留这一点探索意图，并把希望寄托于未来，因此把它作为附录放在原来第五章的位置.

二、讲抽象群、环、域理论的同时，较深入地介绍一些具体群、具体环和具体域. 在本教程中我们选择了变换群（包括运动群、置换群），这里没有足够的篇幅谈论矩阵群是一个遗憾. 对域论，我们选择了多项式的分裂域——Galois 理论，对环论，选择了复数域上多元多项式环——Gröbner 基理论. 这些具体的群、环、域不但有助于我们学习抽象理论，同时也使我们看到代数的一些应用：平面有限对称图形的分类，几何作图不能问题，根式解五次方程不能问题，编码问题，初等几何的机器证明等.

三、关于群、环、域、模都有彼此类似的基本概念：子系统（子群、子环、子域、子模），商系统（商群、商环、商模），同态和同构等等，以及作为它们的支柱

的一些具体例子，这些是代数的基础. 当然还要对群、环、域、模中的每一个至少选择一个较深入的结构定理，否则内容将是散漫的而无重心和方向. 对环论，我们选择了整除理论和 Gröbner 基理论. 对域论，是分裂域理论——Galois 理论. 对群论，是 Sylow 定理和有限交换群的结构定理，而且强调了后者，这不仅是因为它是一个典型结构定理(分解定理)，而且也顺便为模论提供了一个好的结果.

四、一个好的数学思想是一定会在不同场合下重复出现的. 使初学者能看到这些重复是有益的. 在本教程中分解型结构思想重复出现在有限交换群的结构定理和代数簇的分解定理中，当然它们又都是整数和一元多项式的唯一分解一脉相承的. Galois 对应思想重复出现在 Galois 理论中和代数簇和理想的对应中.

五、本教材中我们对基本内容努力写得细致一些，这使得读者甚至可以自学. 同时在某些适当的地方粗略(略去证明)介绍一些进一步的情况，好像在爬山到达一定高度时，停下来欣赏一下周围的景色，这对提高游兴是有益的. 然而用这种方式去介绍五次方程不能用根式解问题是一种不得已！ 它太重要了，不能略去；另一方面无法(没有学时)把它作为基本内容放在本基础课中.

六、本教材的基本内容也就是我们认为抽象代数基础课应该提供给数学专业学生的必需内容. 也许有的材料(如自由群或 Gröbner 基等)没有时间去讲，然而在教材中提供方便，使得读者有机会知道这些内容是应该的. 但无论如何，内容和学时之间是有矛盾的. 也许可由任课教师选讲其中部分章节，也许采用傅种孙教授提倡的讲法：讲重点，讲难点，讲思路，讲体会，利用本教材写得较细致的方便而把基本推导留给学生自学，这样“精讲”加“自学”的方式能完成主要内容的学习.

七、习题是重要的. 我们认识到，学一门课的同时，作一个有代表性的较系统的大习题(学年作业)是非常有益的. 在有限交换群的结构定理之后，我们布置了矩阵的 Jordan 标准型的模论证法以及主理想整环上有限生成周期模的结构定理的证明这样的大习题. 我们相信，相对独立地完成这个大习题的读者定会对本基础课有较亲切的理解而受益匪浅.

我于 1996 年冬至 1997 年夏完成初稿，1997 年秋至 1998 年夏在山东大学等几所大学试用. 1998 年秋，四川大学、厦门大学和北京师范大学参加试用的教师们在北京作了逐章逐节的讨论和修改，最后由彭联刚(四川大学)和林亚南(厦门大学)执笔完成并编写了习题. 书中有关用计算机计算的例子都是罗运伦同志提供的. 这样，这本书实际上是一个集体作品.

在本书中,作者常在一些地方和读者交流体会和理解,有时提到一些补充资料.这些不属于正文的"旁白"都用楷体字排出.

作者特别感谢两届系领导黄惟明、余玄冰以及张英伯、何青等同志,没有他们的推动与鼓励,这本书是不可能出现的.感谢审稿人石生明教授,他仔细地审阅全书,指出若干疏漏和该改进的地方,提出了建议,为本书增色许多.继过去在代数数论教材编审小组的长期共事,这次与责任编辑张小萍同志的再度合作,特别使我感到愉快。感谢石生明同志和张小萍同志,是在他俩的建议下,我在最后时刻写出了编码这一节.在近世代数教科书中介绍一点编码——代数学的一个最直接而重要的应用,是自然的和必要的.读者会喜欢它的.

本书荣幸地得到北京师范大学、四川大学、厦门大学三校教务处,天元基金委,教育部"面向21世纪教学内容和课程体系改革"项目以及普通高等教育"九五"国家重点教材项目的资助,在此作者表示衷心的感谢.

限于作者水平,书中定有许多不妥的地方,敬请读者指正.

刘绍学

1998年12月于北京师大

目　录

第一章　对称与群 …… (1)
§1　平面的运动群 …… (1)
§2　数域的对称 …… (4)
§3　多项式的对称 …… (8)
第二章　群 …… (12)
§1　群 …… (12)
§2　子群 …… (17)
§3　生成元集,循环群 …… (22)
§4　子群(续) …… (28)
§5　商群 …… (32)
§6　同态 …… (38)
§7　有限群 …… (42)
§8　有限交换群的结构定理 …… (46)
§9　单群 …… (53)
§10　群的构造,自由群 …… (58)
§11　群在集上的作用 …… (65)
第三章　环、域与模 …… (73)
§1　环与域 …… (73)
§2　环的构造 …… (83)
§3　多项式环 …… (92)
§4　交换环 …… (98)
§5　整环的整除理论 …… (105)
§6　环的表示与模 …… (116)
第四章　多项式的分裂域 …… (125)
§1　域 …… (125)
§2　分裂域 …… (130)
§3　有限域(分裂域的一个应用) …… (135)
§4　正规扩域(分裂域续) …… (137)

§5 Galois 基本定理 …… (142)
§6 一个例子 …… (149)
§7 尺规作图不能问题 …… (154)
§8 用根式解代数方程问题 …… (157)
§9 有限域的一个应用——编码 …… (161)
附录 多元多项式环(代数几何初步) …… (169)
§1 代数簇 …… (169)
§2 Hilbert 基定理 …… (172)
§3 代数簇的分解 …… (175)
§4 Gröbner 基 …… (179)
§5 Buchberger 算法 …… (185)
§6 初等几何的机器证明 …… (190)
参考书目 …… (195)
符号表 …… (196)
名词索引 …… (197)

第一章　对称与群

抽象代数是以群、环、域、模为主要研究对象的学科.本章将引进群(带有一个二元运算的集合)的概念,并特别强调群这一概念出现的背景.学习完本章后,我们期望读者能对“对称即群”有一个初步但明确的理解.

§1　平面的运动群

我们来探讨平面上有限图形的对称问题.人们都会说圆比正方形更对称些,正六边形比正三角形更显得对称一些.如果问正三角形和正方形谁更对称一些,该怎么回答呢?

看来要把图形的对称这个直观概念说得确切一些,也就要给它一个定义,一个反映客观实际,能为大家接受的定义.

有某种对称的图形,就是经过某些运动后仍能回到自身的图形.例如,圆经过绕圆心的旋转以及绕过圆心的直线的翻摺都是回到自身,而正方形只能绕其中心旋转 $\frac{\pi}{2},\pi,\frac{3}{2}\pi$ 或绕其对角线或对边中点连线所作的翻摺才能回到自身,也许这就是圆比正方形更对称一些的解释.用使图形回到自身的所有运动来刻画这一图形的对称应该是自然的,也符合我们对对称的直观感觉.

在这里我们回忆一下平面及其运动的概念.

用朴素平面几何的说法,可把平面想象为可向各方无限延伸的黑板面,我们还有平面上的点及两点距离的概念.用解析几何的说法,平面就是集合 $\mathbb{R}^2=\{(x,y)\mid x,y\in\mathbb{R}\}$,其中 $\mathbb{R}$ 是实数域,以及点 $A=(a_1,a_2)$, $B=(b_1,b_2)$ 之间的距离 $|AB|=\sqrt{(a_1-b_1)^2+(a_2-b_2)^2}$.(用线性代数的语言,平面也就是二维欧氏空间.)今后我们把关于平面 P 的这两种刻画——几何直观的刻画和代数语言的刻画——等同起来.

定义 1.1　M 是任意一个非空集合, M 的变换是指 M 到自身的一个对应. M 的一一变换是指 M 到自身上的一一对应.

定义 1.2　(几何的定义)　平面 P 的一个运动是指平面 P 的一个保距变换.亦即若 ϕ 是平面 P (点集)的一个变换,且对 P 上任意点 A 和点 B, $\phi(A)$ 和 $\phi(B)$ 的距离等于 A 和 B 的距离,则称 ϕ 为平面 P 的一个运动.易见平面 P 的运动是 P 的一一对应.

由线性代数中欧氏空间的理论,我们有下面

定理 1.3a (代数的形式) 平面 $\mathbb{R}^2$ 的一个运动,是且仅是 $\mathbb{R}^2$ 中具有下面形式的变换

$$\begin{aligned}\phi:\quad \mathbb{R}^2 &\longrightarrow \mathbb{R}^2\\ (x,y) &\longmapsto (x',y'),\end{aligned}$$

且
$$\begin{pmatrix}x'\\y'\end{pmatrix}=O\begin{pmatrix}x\\y\end{pmatrix}+\begin{pmatrix}a_1\\a_2\end{pmatrix},$$

其中 O 是 2×2 正交矩阵, $A=(a_1,a_2)^T$ 是一个取定的向量.

利用平面几何的方法,或把平面几何和上述定理结合起来,可以证明下面著名的结果.

定理 1.3b (几何的形式,M. Chasles (1793—1880)) 平面的运动有且只有下列三种:

a) 沿任一给定向量的平移;

b) 以任意点为中心的旋转;

c) 绕某一直线作翻摺后再沿该直线上的一个向量作一平移(包括作纯翻摺的情况).

我们还知道,在定理 1.3a 中当 $A=(0,0)^T$ 而 $\det|O|=1$ 时,运动 ϕ 就是绕原点的旋转;而当 $A=(0,0)^T$ 且 $\det|O|=-1$ 时, ϕ 就是以某一过原点的直线为轴的翻摺;而 $O=E$ (单位矩阵)时, ϕ 就是沿向量 $A=(a_1,a_2)^T$ 的平移.

对我们来说非常重要的是,两个变换是可以相乘的,这就是

定义 1.4 M 是一个非空集合, ϕ 和 ψ 是 M 的两个变换.规定 M 到自身的映射 $\rho(x)=\phi(\psi(x))$ (对任意 $x\in M$),则易知 ρ 是 M 的变换.我们定义 ρ 是变换 ϕ 和变换 ψ 的乘积,记作 $\rho=\phi\circ\psi$.注意到 M 的两个一一变换的乘积仍是一个一一变换,我们特把 M 的一一变换全体记作 $T(M)$,并把映射

$$\begin{aligned}\circ:\quad T(M)\times T(M) &\longrightarrow T(M)\\ (\phi,\psi) &\longmapsto \phi\circ\psi\end{aligned}$$

称为 $T(M)$ 的一个乘法.

我们知道,变换的乘法适合结合律,即 $(\phi\circ\psi)\circ\theta=\phi\circ(\psi\circ\theta)$.

我们还知道恒等变换 I (即把 M 的每一元素 x 对应到 x 本身的变换)是 M 的一一变换, M 的一一变换 ϕ 的逆变换 ϕ^{-1} 是 M 的一一变换,以及 $\phi\circ\phi^{-1}=\phi^{-1}\circ\phi$ 是恒等变换 I.

定义 1.5 M 是一个非空集合, $T(M)$ 是 M 的所有一一变换的全体.我

们把 $T(M)$ 以及变换的乘法放在一起来考察,记作 $(T(M),\circ)$(这里 $\circ$ 表示变换的乘法),并称之为 M 的变换群.

这里再强调一下,我们并不是把集 $T(M)$ 叫作变换群,而是把带有乘法运算的 $(T(M),\circ)$ 叫作变换群.代数学的特点是研究带有运算的集合.对于一个集合,只有在其中引入运算后,才是代数学研究的对象.

把上面提到的已知事实总结一下便有下面的

命题 1.6 变换群 $(T(M),\circ)$ 具有下列性质:

G1) 对任意 $\phi,\psi\in T(M)$,有 $\phi\circ\psi\in T(M)$;

G2) 对任意 $\phi,\psi,\theta\in T(M)$,有 $(\phi\circ\psi)\circ\theta=\phi\circ(\psi\circ\theta)$;

G3) 存在 $I\in T(M)$ 使得对任意 $\phi\in T(M)$,有 $I\circ\phi=\phi\circ I=\phi$;

G4) 对任意 $\phi\in T(M)$,存在 $\phi^{-1}\in T(M)$,使得 $\phi\circ\phi^{-1}=\phi^{-1}\circ\phi=I$. □

现在我们从一般集 M 及其一一变换回到平面 $\mathbb{R}^2$ 及其运动上来.

用 $M(\mathbb{R}^2)$ 表示平面 $\mathbb{R}^2$ 的所有运动,运动只不过是特殊(保距)的一一变换,即有 $M(\mathbb{R}^2)\subseteq T(\mathbb{R}^2)$,后者是 $\mathbb{R}^2$ 的所有一一变换的全体.很容易证明:平面的两个运动(保距变换)的乘积仍是一个运动,一个运动 ϕ 的逆变换 ϕ^{-1} 仍是一个运动.当然恒等变换是一个保距变换.这样我们就得到

命题 1.7 $M(\mathbb{R}^2)$ 对于变换的乘法具有下列性质:

G1) 对任意 $\phi,\psi\in M(\mathbb{R}^2)$,有 $\phi\circ\psi\in M(\mathbb{R}^2)$;

G2) 此时当然对任意 $\phi,\psi,\theta\in M(\mathbb{R}^2)$,有 $(\phi\circ\psi)\circ\theta=\phi\circ(\psi\circ\theta)$;

G3) 恒等变换 $I\in M(\mathbb{R}^2)$.此时当然对任意 $\phi\in T(M)$,有 $I\circ\phi=\phi\circ I=\phi$;

G4) 对任意 $\phi\in M(\mathbb{R}^2)$,也有 $\phi^{-1}\in M(\mathbb{R}^2)$,此时当然也有 $\phi\circ\phi^{-1}=\phi^{-1}\circ\phi=I$. □

很自然地,我们该有下面的

定义 1.8 称 $(M(\mathbb{R}^2),\circ)$ 为平面 $\mathbb{R}^2$ 的运动群,这里 $\circ$ 表示运动的乘法(也就是变换的乘法).

现在来考察使平面图形 K 仍回到自身的平面运动的全体,把它记作 $S(K)$.我们知道,平面图形 K 也就是平面 $\mathbb{R}^2$ 上一些点的集合,即 $K\subseteq\mathbb{R}^2$,且 K 中任意两点间有距离;而使 K 保持不变的运动也就是使 $\phi(K)=K$ 的运动 ϕ(这里 $\phi(K)=\{\phi(x),x\in K\}$).

定义 1.9 我们把 $S(K)$ 称作平面图形 K 的对称.

这样,我们就把图形 K 的直观对称的概念用精确的数学语言——集合 $S(K)$ 来刻画:K 的对称就是集合 $S(K)$.我们当然无法“证明”,这个 $S(K)$ 就是你心目中的对称,$S(K)$ 只是我们心目中直观对称概念的一个数学模

型.然而从实践上来看,这个数学模型是可接受的,是好的.读者容易证明下面

命题 1.10 $(S(K),\circ)$ 满足上面命题中的 G1)–G4)这四个条件.□

定义 1.11 我们称 $(S(K),\circ)$ 为平面图形 K 的对称群.

例 1 正方形的对称群是由下列平面运动组成:恒等运动,绕其中心转 $90°,180°,270°$ 的旋转,以及关于它的两条对角线,两条对边中点连线所作的翻摺.一共 8 个运动.

很容易验证这 8 个运动,使正方形仍回到自身上去.另一方面利用 Chasles 定理可得其它的平面运动都不使该正方形回到自身,故得上述结果.

由于图形的对称性可由对称群这一代数对象来刻画,下一步我们就可用代数方法去研究图形的对称,这有点儿像笛卡尔坐标系把几何图形和方程式联系起来后,我们在解析几何中可用代数方法研究几何一样.不同的是在解析几何中我们用的是多项式,而这一次是用"群"了.

关于图形,以至晶体的对称群的研究请看相应的参考书.

练习

1. 设 ϕ 是平面 $\mathbb{R}^2$ 的一个运动,其代数形式为

$$\begin{array}{cccc}\phi: & \mathbb{R}^2 & \longrightarrow & \mathbb{R}^2\\ & (x,y) & \longmapsto & (x',y'),\end{array}$$

满足 $\begin{pmatrix}x'\\y'\end{pmatrix}=O\begin{pmatrix}x\\y\end{pmatrix}$,其中 O 是 $\mathbb{R}$ 上一个 2×2 正交矩阵.证明:如果 $\det|O|=-1$,那么存在一条直线 l,使得运动 ϕ 是关于直线 l 的对称变换,即对任意 $A=(x,y)\in\mathbb{R}^2$,有 $\phi(A)=(x',y')\in\mathbb{R}^2$ 是 A 的关于直线 l 的对称点,从而 ϕ 是绕 l 的翻摺.

2. 设 M 是一个非空集合.证明:变换群 $(T(M),\circ)$ 满足结合律,即命题 1.6 中的 G2).

3. 设 K 是正六边形.写出 K 的对称群 $S(K)$.

§2 数域的对称

先回忆一下在高等代数中学过的数域的概念.

我们假定复数以及其加法、减法、乘法是大家都熟悉的.令 $\mathbb{C}$ 表示复数全体.

定义 2.1 称 $\mathbb{C}$ 的一个含有 0 和 1 的子集 F 为一个数环,如果 F 满足下列条件

F1) F 关于数的加法、减法和乘法是封闭的,即若 $a,b\in F$,则 $a+b$, $a-b$, $a\cdot b$ 都在 F 中;

如果除 F1)外 F 还满足

F2) 若 $0 \neq a \in F$ 则 a 的逆元 a^{-1} 也在 F 中,
则称 F 为一个数域.

显然,全体非负整数不是数环,而全体整数是数环但不是数域,全体有理数、全体实数都是数域.

例 1 $F = \{a + b\sqrt{2} \mid a, b \text{ 是有理数}\}$ 是数域.

平面图形是一个几何结构,即是把一个点集 M 连同此点集 M 中任意两点间有距离作为一个整体来考虑,而其对称群就是 M 的保持其任两点间距离的变换的全体,这些保持 M 的几何结构(即距离)的变换的全体,就刻画了几何结构的对称.

完全类似地,数域 F 是一个代数结构,即是把一个数集 F 连同此数集 F 中加、减、乘的运算作为一个整体一起来考虑.数域 F 的对称也同样地可用 F 的保持代数结构(即运算)的变换的全体来刻画,虽然它不像图形对称那样直观,但它是客观存在的.这样我们有下面的

定义 2.2 数域 F 的自同构 ϕ 是指

a) ϕ 是集合 F 到 F 上的一个一一对应(即 F 的一一变换);

b) 对所有 $x, y \in F$ 有:$\phi(x + y) = \phi(x) + \phi(y), \phi(xy) = \phi(x)\phi(y)$.

在定义中我们没有要求自同构保持 F 中的减法运算和取逆,这是因为它们是保持加法和乘法的推论:

命题 2.3 设 ϕ 是数域 F 的自同构,则有

1) $\phi(0) = 0, \phi(1) = 1$;

2) 对任意 $x, y \in F$, 有 $\phi(-x) = -\phi(x), \phi(x - y) = \phi(x) - \phi(y)$;

3) 对任意 $0 \neq x \in F$, 有 $x^{-1} \in F$, 使 $\phi(x^{-1}) = \phi(x)^{-1}$.

证明 1) 依定义 2.2 中 b), 有 $\phi(0) = \phi(0+0) = \phi(0) + \phi(0)$, 从两侧消去 $\phi(0)$ 便得 $\phi(0) = 0$. 同样方法可证 $\phi(1) = 1$.

2) 依 1)及定义 2.2 中 b), 有 $0 = \phi(0) = \phi(x + (-x)) = \phi(x) + \phi(-x)$, 故 $\phi(-x) = -\phi(x)$. 随之也有

$$\begin{aligned}\phi(x - y) &= \phi(x + (-y)) = \phi(x) + \phi(-y) \\ &= \phi(x) + (-\phi(y)) = \phi(x) - \phi(y).\end{aligned}$$

3) 用同样方法可证.□

和 §1 中两个保持几何结构的运动的乘积仍是保持该几何结构的运动完全类似的,我们有

命题 2.4 设 ϕ,ψ 是数域 F 的两个自同构,则 $\phi^{-1},\phi\psi$ 也都是数域 F 的自同构.

证明 由于数域 F 的自同构首先是集 F 的变换,故 $\phi^{-1},\phi\psi$ 的意义是清楚的,它们都是集 F 的变换.

先证 $\phi\psi$ 是自同构. 任取 $x,y\in F$,则依变换乘积的定义有

$$(\phi\psi)(xy)=\phi(\psi(xy))=\phi(\psi(x)\psi(y))$$
$$=\phi(\psi(x))\cdot\phi(\psi(y))=(\phi\psi)(x)\cdot(\phi\psi)(y).$$

类似地可证 $\phi\psi$ 保持加法.

再证 ϕ^{-1} 是自同构. 任取 $x,y\in F$. 由于 ϕ 是 F 到 F 上的一一对应,故必有 $x',y'\in F$ 使得 $x=\phi(x'),y=\phi(y')$. 此时当然也有 $x'=\phi^{-1}(x),y'=\phi^{-1}(y)$. 这样就有

$$\phi^{-1}(xy)=\phi^{-1}(\phi(x')\phi(y'))=\phi^{-1}(\phi(x'y'))=x'y'=\phi^{-1}(x)\phi^{-1}(y).$$

类似地可证 ϕ^{-1} 保持加法. □

从以上命题,我们便有

定理 2.5 令 $\mathrm{Aut}(F)$ 表示数域 F 的所有自同构的全体,令 $\circ$ 表示变换的乘法,则 $(\mathrm{Aut}(F),\circ)$ 具有下列性质

G1) 对任意 $\phi,\psi\in\mathrm{Aut}(F)$,有 $\phi\circ\psi\in\mathrm{Aut}(F)$;

G2) 对任意 $\phi,\psi,\theta\in\mathrm{Aut}(F)$,有 $(\phi\circ\psi)\circ\theta=\phi\circ(\psi\circ\theta)$;

G3) 存在 $I\in\mathrm{Aut}(F)$ 使得对任意 $\phi\in\mathrm{Aut}(F)$,有 $I\circ\phi=\phi\circ I=\phi$;

G4) 对任意 $\phi\in\mathrm{Aut}(F)$,存在 $\phi^{-1}\in\mathrm{Aut}(F)$ 使得 $\phi\circ\phi^{-1}=\phi^{-1}\circ\phi=I$.

易见上面 G3)中的 I 就是 F 的恒等变换:对任意 $x\in F$,有 $I(x)=x$. 称之为恒等自同构. □

定义 2.6 我们称 $(\mathrm{Aut}(F),\circ)$ 为数域 F 的自同构群.

这里我们再作一次类比:数域 F 的自同构群相当于图形 K 的对称群,后者刻画了图形 K 的对称,前者则刻画了数域的“对称”——它是图形对称在数域上的一个类比概念.

例 2 有理数域 $\mathbb{Q}$ 的自同构群只有一个元素——恒等自同构 I.

这是因为,任取 $\mathbb{Q}$ 的一个自同构 ϕ,由 $\phi(1)=1$ 得 $\phi(2)=\phi(1+1)=\phi(1)+\phi(1)=2$,一般对任意正整数 n 有 $\phi(n)=n$,随之 $\phi(-n)=-\phi(n)=-n$,$\phi(1/n)=\phi(n^{-1})=\phi(n)^{-1}=n^{-1}$. 故对任意整数 n,m 我们有 $\phi(m/n)=\phi(m)\phi(1/n)=m\cdot 1/n=m/n$. 即 $\phi=I$. □

从上面证明中,可知对任意数域 F(它当然包含所有有理数)的自同构 ϕ 必有 $\forall x\in\mathbb{Q}$, $\phi(x)=x$.

例 3 令 $F=\mathbb{Q}(\sqrt{2})=\{a+b\sqrt{2},|,a,b\in\mathbb{Q}\}$,易验证 F 是一个数域.

今考察 F 的自同构群. 任取 F 的自同构 ϕ, 注意到 $\forall a \in \mathbf{Q}$, $\phi(a)=a$, 故有 $\phi(a+b\sqrt{2})=\phi(a)+\phi(b)\phi(\sqrt{2})=a+b\cdot\phi(\sqrt{2})$. 这样只要 $\sqrt{2}$ 在 ϕ 下的象 $\phi(\sqrt{2})$ 定了,则 ϕ 也就完全确定了. ϕ 是自同构,是保持运算的,故 $\sqrt{2}$ 所适合的有理系数代数关系式, $\phi(\sqrt{2})$ 也应该适合,特别 $\sqrt{2}$ 是 $x^2-2=0$ 的根,即 $(\sqrt{2})^2-2=0$, 故由

$$0=\phi(0)=\phi((\sqrt{2})^2-2)=\phi(\sqrt{2})^2-2$$

也知 $\phi(\sqrt{2})$ 是 $x^2-2=0$ 的根. 因而 $\phi(\sqrt{2})$ 的可能值最多只有两个: $\sqrt{2}$ 和 $-\sqrt{2}$. 直接验证

$$I:\ F \longrightarrow F \qquad \phi:\ F \longrightarrow F$$
$$a+b\sqrt{2} \longmapsto a+b\sqrt{2}, \qquad a+b\sqrt{2} \longmapsto a-b\sqrt{2}$$

确是数域 F 的自同构. 这样, F 的自同构群是 $\{I,\phi\}$, 其乘法是 $II=I, I\phi=\phi I=\phi$, $\phi\phi=I$, 或可写成如下的乘法表

$\circ$	I	ϕ
I	I	ϕ
ϕ	ϕ	I

例 4 令 $E=\mathbf{Q}(\sqrt{2},\sqrt{3})=\{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{2}\sqrt{3} \mid a,b,c,d \in \mathbf{Q}\}$. 易验证 E 是一个数域. 和例 3 完全类似,如果 ϕ 是 E 的自同构,则 ϕ 完全由 $\phi(\sqrt{2})$ 和 $\phi(\sqrt{3})$ 确定,而 $\phi(\sqrt{2})$ 的可能值只有 $\sqrt{2}$ 和 $-\sqrt{2}$, $\phi(\sqrt{3})$ 的可能值只有 $\sqrt{3}$ 和 $-\sqrt{3}$. 直接验证,可知下列变换都是数域 E 的自同构:

$$I:\ a+b\sqrt{2}+c\sqrt{3}+d\sqrt{2}\sqrt{3} \longmapsto a+b\sqrt{2}+c\sqrt{3}+d\sqrt{2}\sqrt{3}$$
$$\phi_1:\ a+b\sqrt{2}+c\sqrt{3}+d\sqrt{2}\sqrt{3} \longmapsto a-b\sqrt{2}+c\sqrt{3}-d\sqrt{2}\sqrt{3}$$
$$\phi_2:\ a+b\sqrt{2}+c\sqrt{3}+d\sqrt{2}\sqrt{3} \longmapsto a+b\sqrt{2}-c\sqrt{3}-d\sqrt{2}\sqrt{3}$$
$$\phi_{12}:\ a+b\sqrt{2}+c\sqrt{3}+d\sqrt{2}\sqrt{3} \longmapsto a-b\sqrt{2}-c\sqrt{3}+d\sqrt{2}\sqrt{3}$$

这样, E 的自同构群是 $\{I,\phi_1,\phi_2,\phi_{12}\}$, 其乘法表为

$\circ$	I	ϕ_1	ϕ_2	ϕ_{12}
I	I	ϕ_1	ϕ_2	ϕ_{12}
ϕ_1	ϕ_1	I	ϕ_{12}	ϕ_2
ϕ_2	ϕ_2	ϕ_{12}	I	ϕ_1
ϕ_{12}	ϕ_{12}	ϕ_2	ϕ_1	I

表中 x - 行 y - 列交叉处的元素等于 $x \circ y$, 例如 $\phi_1 \circ \phi_2 = \phi_{12}$ 等等. 常称这样的表为 Cayley 表, 以示人们对为群论作出贡献的 A. Cayley(英国数学家, 1821—1895)的敬意.

给两个数域 F 和 E, 如果有 $F \subseteq E$, 我们称 F 是 E 的子域, 而称 E 为 F 的扩域.

对给定的两个数域 F 和 E, $F \subseteq E$. 令

$$\mathrm{Aut}(E:F) = \left\{\phi \in \mathrm{Aut}(E) \,\middle|\, \forall x \in F, \phi(x) = x\right\},$$

即它的元素是那些使得 F 中元素不动的, 数域 E 的自同构.

命题 2.7　$(\mathrm{Aut}(E:F), \circ)$ 满足定理 2.5 中的性质 G1)—G4). □

定义 2.8　我们称 $(\mathrm{Aut}(E:F), \circ)$ 为数域 E 在 F 上的对称群.

当然, 一般说 $\mathrm{Aut}(E:F)$ 是 $\mathrm{Aut}(E)$ 的一个真子集, 它不再刻画数域 E 的对称, 它刻画的是数域 E 的保持 F 中元素不动的那种对称性. 我们将在下一节中看到这种对称性的意义.

取上面例 3 中的 $F = \mathbb{Q}(\sqrt{2})$, 例 4 中的 $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, 则我们有 $\mathbb{Q} \subseteq F \subseteq E$. 关于这些数域, 有下面结果.

例 5　$\mathrm{Aut}(E:\mathbb{Q}) = \mathrm{Aut}(E) = \{I, \phi_1, \phi_2, \phi_{12}\}$.

例 6　$\mathrm{Aut}(E:F) = \{I, \phi_2\}$. 这是因为自同构 ϕ_1, ϕ_{12} 使 F 中的有些数不对应本身.

练习

1. 证明: $F = \left\{a + b\sqrt{2} \,\middle|\, a, b \in \mathbb{Q}\right\}$ 是数域.

2. 设 F 是数域. 证明: $\mathrm{Aut}(F:\mathbb{Q}) = \mathrm{Aut}(F)$.

3. 设 a, b, c, d 为有理数. 证明: 如果 $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3} = 0$, 那么 $a = b = c = d = 0$.

4. 设 $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$ 和 $\mathbb{Q}(i, \sqrt{5}) = \{a + bi + c\sqrt{5} + di\sqrt{5} \mid a, b, c, d \in \mathbb{Q}\}$.

　1) 证明: $\mathbb{Q}(i)$ 和 $\mathbb{Q}(i, \sqrt{5})$ 是域.

　2) 若记 $F = \mathbb{Q}(i), E = \mathbb{Q}(i, \sqrt{5})$, 求 $\mathrm{Aut}(F), \mathrm{Aut}(E)$ 和 $\mathrm{Aut}(E:F)$. 并写出 $\mathrm{Aut}(E)$ 的乘法表.

§3　多项式的对称

我们都熟悉 n 个变元 $x_1, x_2, \cdots, x_n$ 的 n 元多项式. 今把以数域 F 中的数作系数的 n 元多项式的全体记作 $F[x_1, x_2, \cdots, x_n]$ (或简记作 $F[X]$), 每一 n 元多项式可以唯一地表示为不同类单项式的有限线性和:

$$f(x_1,x_2,\cdots,x_n)=\sum_{\alpha}a_{\alpha}x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n},$$

其中 $\alpha=(\alpha_1,\alpha_2,\cdots,\alpha_n)$，$\alpha_i\in\mathbb{Z}^+\cup\{0\}$，而 $a_\alpha\in F$.

令 $M=\{x_1,x_2,\cdots,x_n\}$. 用 S_n 表示集合 M 的变换群(见§1). S_n 常称作 n 元对称群. S_n 中的元素就是 $\{x_1,x_2,\cdots,x_n\}$ 的一个置换，略去字母 x 而只记下标，这时的置换可记作

$$\Sigma=\begin{pmatrix}1 & 2 & \cdots & n\\ i_1 & i_2 & \cdots & i_n\end{pmatrix},$$

其中 $(i_1,i_2,\cdots,i_n)$ 是 $1,2,\cdots,n$ 的一个排列，而 $\Sigma(j)=i_j$.

现在我们利用变换群 S_n 中的元素 Σ 去定义集合 $F[X]$ 到 $F[X]$ 的一个映射

$$\begin{aligned}\phi_\Sigma:\quad F[X] &\longrightarrow F[X]\\ f(x_1,x_2,\cdots,x_n) &\longmapsto f(x_{i_1},x_{i_2},\cdots,x_{i_n}),\end{aligned}$$

其中 $f(x_{i_1},x_{i_2},\cdots,x_{i_n})$ 是在多项式 $f(x_1,x_2,\cdots,x_n)$ 中将 x_1 换成 x_{i_1}，x_2 换成 x_{i_2}，… 后所得到的多项式.

不难证明这是集 $F[X]$ 的一个变换. 这实际上就是把其子集 $\{x_1,x_2,\cdots,x_n\}$ 的一个变换 Σ 用一种“自然方式”扩大成为整个集合 $F[X]$ 的一个变换 ϕ_Σ.

令 $T_n=\{\phi_\Sigma\mid\Sigma\in S_n\}$. T_n 是 $F[X]$ 的一些($n!$ 个)变换组成的集合. 注意到(请读者证明一下)

$$\phi_\Sigma\circ\phi_\theta=\phi_{\Sigma\circ\theta},\quad(\phi_\Sigma)^{-1}=\phi_{\Sigma^{-1}}.$$

我们有

命题 3.1 $(T_n,\circ)$ 满足性质 G1)—G4)，称之为 $F[X]$ 的置换群.

如果把 n 元多项式和平面图形类比，把 $F[X]$ 和平面类比，则 $F[X]$ 的置换群相当于平面的运动群.

定义 3.2 令 $f(x_1,x_2,\cdots,x_n)$ 是一个 n 元多项式，令

$$S_f=\{\phi_\Sigma\in T_n\mid\phi_\Sigma(f)=f\}.$$

命题 3.3 $(S_f,\circ)$ 满足性质 G1)—G4). 称之为 n 元多项式 $f(x_1,x_2,\cdots,x_n)$ 的对称群.

例 1 $F[x_1,x_2,x_3,x_4]$ 中的多项式 $f=x_1x_2+x_3x_4$ 的对称群

$$S_f=\left\{\phi_\Sigma\,\middle|\,\Sigma=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix},\right.$$

$$\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix},\begin{pmatrix}1&2&3&4\\4&3&1&2\end{pmatrix},$$

$$\begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix},\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}\Bigg\}.$$

定义 3.4 $F[x_1,x_2,\cdots,x_n]$ 中的一个 n 元多项式 f 叫做对称多项式，如果 $S_f = T_n$，即其对称群是整个置换群 T_n.

这就是我们熟悉的对称多项式的定义.

上面是从形式上考虑多元多项式的对称性，下面我们考察一元多项式的根的对称性，这可以看作是从"内容"的角度考虑一元多项式的对称性.

设 F 是一取定的数域，$F[x]$ 表示系数在 F 中的一元多项式的全体.我们熟悉 $F[x]$ 中一元多项式之间的加法、减法和乘法运算.任取 $F[x]$ 中的一个首项系数为 1 的 n 次多项式 $f(x)$，则根据代数基本定理知 $f(x)$ 在复数域 $\mathbb{C}$ 有 n 个根，记作 $\alpha_1,\alpha_2,\cdots,\alpha_n$；其中可能有相同者，但我们把它们用不同的符号表示.这时我们当然有

$$f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n).$$

我们把这些根 α_i 和系数域 F 放在一起，并设法在 $\mathbb{C}$ 中找到一个包含 α_i 和 F 的尽可能小的（因为现在我们只对这些根 α_i 和 F 感兴趣）的数域.由于数域对加、减、乘、除（除数不为 0）是封闭的，故这个数域必包含下面数集

$$E = \left\{\frac{g(\alpha_1,\alpha_2,\cdots,\alpha_n)}{h(\alpha_1,\alpha_2,\cdots,\alpha_n)}\,\middle|\, g,h\in F[x_1,x_2,\cdots,x_n]\right.$$

$$\left.\text{且}\quad h(\alpha_1,\alpha_2,\cdots,\alpha_n)\neq 0\right\}.$$

另一方面，数集 E 中任意两个数，它们经过加、减、乘、除（除数不为 0）后仍然具有 $g(\alpha_1,\alpha_2,\cdots,\alpha_n)/h(\alpha_1,\alpha_2,\cdots,\alpha_n)$ 的形式，故仍在 E 中.例如，把 $g(\alpha_1,\alpha_2,\cdots,\alpha_n)$ 简记作 $g(\alpha)$ 时，我们有

$$\frac{g_1(\alpha)}{h_1(\alpha)}+\frac{g_2(\alpha)}{h_2(\alpha)}=\frac{g_1(\alpha)h_2(\alpha)+h_1(\alpha)g_2(\alpha)}{h_1(\alpha)h_2(\alpha)}=\frac{g_3(\alpha)}{h_3(\alpha)},$$

其中 $g_3(\alpha)=g_1(\alpha)h_2(\alpha)+h_1(\alpha)g_2(\alpha)$，$h_3(\alpha)=h_1(\alpha)h_2(\alpha)$，故 E 中两元素之和仍在 E 中.同样地可证其他情形.

这样数域 E 是包含 F 和诸 α_i 的最小数域.我们常称 E 为把诸根 α_i 添加到 F 上得到的数域，也称 E 为多项式 $f(x)$（$\in F[x]$）在数域 F 上的分裂域，因为当把 $f(x)$ 看作 $E[x]$ 中多项式时，有

$$f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n),$$

即 $f(x)$ 在 $E[x]$ 中完全分解为一次多项式的乘积.下面常把 E 记作 $E = F(\alpha_1,\alpha_2,\cdots,\alpha_n)$.

定义 3.5 F,f,E 的意义如上.称 $(\mathrm{Aut}(E:F),\circ)$ 为 F 上一元多项式 f 的根的对称群，也称之为 F 上一元多项式 f 的 Galois 群.

我们可以认定（Aut($E:F$)，∘）是刻画 $f(x)$ 的根的对称性的. 多项式的根的对称性不像图形的对称性那样直观，那样具体，然而如果你仔细体会一下上面的讨论，诸如：根是一些数，它们之间有代数结构，也就是有运算关系；和考虑多项式的形式上对称不同，必须考虑根之间的代数关系；E 这个数域概括了根之间的全部代数关系，…… 那么，你就能体会到，Aut($E:F$) 的确刻画了根集的对称. 这是法国天才数学家 E. Galois(1811—1832)在 1828 年他 17 岁时，讨论五次方程的代数解法时总结而提出的想法. 在此基础上发展的 Galois 理论，不但彻底解决五次方程不能用根式解的古典问题，更重要的是创立了群论，开辟了代数学的新纪元. 我们将在第四章介绍域的 Galois 理论.

从上面几节可看到对称和群的密切关系. 这里所谈的对称，概括起来说就是：当我们考虑的对象 A 是一个带有若干关系的集合 M（数学中的对象大致都具有这种形式）时，我们就把所有保持这些关系不变的，集 M 的一一变换的全体所构成的群看作是这个对象 A 的对称. 这就是我们前面所用的，非数学术语“对称即群”的内容与含义. 当然事物都在发展中，近来在物理学中讨论更广泛意义的对称性，并用不同于群的数学工具（如 Kac-Moody 代数）去刻画它，则是完全自然的而有益的.

练习

1. 求 $\mathbf{Q}[x_1,x_2,x_3]$ 中多项式 $f = x_1^2 + x_1x_2 + x_2x_3 + x_3^2$ 的对称群 S_f.

2. 设 F 是数域，在 $F[x_1,x_2,x_3]$ 中的所有含有项 $x_1^3x_2$ 的对称多项式中，写出项数最少的那个对称多项式.

3. 设 $f(x,y)$ 是 $\mathbf{R}[x,y]$ 中对称多项式. 证明：在平面 $\mathbf{R}^2$ 中，由方程 $f(x,y) = 0$ 确定的图形 K 关于直线 $l: x - y = 0$ 是对称的.

4. 证明：$f = x^2 - 2$ 在 $\mathbf{Q}$ 上的分裂域是 $E = \{a + b\sqrt{2} \mid a,b \in \mathbf{Q}\}$.

第二章　群

本章介绍群这个抽象代数中最重要的基本概念并作一些基本的讨论.特别提醒读者注意接受和习惯这里的集合论语言和公理化的方法,逐步学会在一个用一组公理定义的对象上推导和思考一些问题,学会把这些抽象对象和具体例子区分开,同时又会把有关抽象对象的结果应用到具体例子上以洞察后者的脉络,还会从具体例子中得到启示或抓住它们的共同点以定义抽象对象并研究它们.

§1　群

前面的变换群、运动群、图形的对称群、多项式的 Galois 群都是具有一个运算的集合,而其中的运算满足我们熟悉的 G1)—G4)诸性质,因而用集合论的语言把它们归纳和概括成一个抽象群的定义,就不是困难的事了.历史上也正是这样:先是 E. Galois 于 1829 引入置换群,C. Jordan 于 1867 引入运动群,之后 A. Cayley 于 1854 及 1878,以及 W. van Dyck 于 1882 给出抽象群的概念.

定义 1.1　M 是个非空集合,称 $M\times M$ 到 M (不必到上)的一个映射 ϕ 为集 M 的一个二元运算.

常把 (x,y) 在 ϕ 的象记成 $x\phi\, y$. 常取 ϕ 为"·",这样 $x\phi y$ 就变成 $x\cdot y$,常称之为 x 和 y 的乘积,这样就和我们通常习惯的符号一致起来了.

类似地,可以定义 3 元运算, n 元运算以及一元运算.也可以定义集合 M 和集合 N 到集合 P 的运算 ϕ, 那就是 $M\times N$ 到 P 的一个映射.

例如:变换的合成(乘法)是集合 $T(M)$ 的一个二元运算;在我们熟悉的数域 F 上向量空间 V 的定义中,数乘运算 $\alpha\cdot x,\alpha\in F,x\in V$ 是集 F 和集 V 到集 V 的一个运算.

定义 1.2　设·是集 S 的一个二元运算.称 $(S,\cdot)$ 为一个半群,如果这个运算满足下列公理:

G1) 对任意 $a,b\in S$, 有 $a\cdot b\in S$;

G2) 对任意 $a,b,c\in S$, 有 $(a\cdot b)\cdot c=a\cdot(b\cdot c)$.

定义 1.3　设·是集合 G 的一个二元运算(我们常称作乘法).称 $(G,\cdot)$ 为一个群,如果这个运算满足下列诸公理:

G1) 对任意 $a,b \in G$, 有 $a \cdot b \in G$;

G2) 对任意 $a,b,c \in G$, 有 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;

G3) 存在 $e \in G$ 使得对任意 $a \in G$, 有 $e \cdot a = a \cdot e = a$;

G4) 对任意 $a \in G$, 存在一元素 $b \in G$, 使 $a \cdot b = b \cdot a = e$;

如果还满足

G5) 对任意 $a,b \in G$, 有 $a \cdot b = b \cdot a$;

则称 $(G, \cdot)$ 为交换群或 Abel 群.

如果群 G 只有有限个元素,称之为有限群,其元素个数称之为群 G 的阶,记为 $|G|$. 除了第一章中看到的变换群、运动群、对称群、Galois 群等都是群外,我们还可以从数、多项式、矩阵或有限维向量空间的线性变换等这些丰富的数学对象中,很容易举出下列例子来.

(全体整数集 $\mathbb{Z}$,数的加法),(非零实数,数的乘法)都是由数及数的运算组成的群的例子;

($\mathbb{Q}$ 中次数 $\leqslant 5$ 的多项式全体,多项式的加法)是群.

以上这些群都是交换群.

($\mathbb{Q}$ 上 n 阶非退化矩阵的全体 $GL_n(\mathbb{Q})$, 矩阵的乘法),($\mathbb{R}$ 上 n 阶正交矩阵的全体 O_n, 矩阵的乘法),($\mathbb{Z}$ 上行列式为 1 的 n 阶矩阵的全体,矩阵的乘法)都是由矩阵及矩阵的运算组成的群的例子.

这些矩阵群不是交换群.

由线性变换及其合成运算组成的群的例子,我们有

($\mathbb{Q}$ 上 n 维线性向量空间 V_n 的非退化线性变换的全体,线性变换的合成运算)是一个群. 仿照第一章 §2 中数域的对称群的说法,它就是 $\mathbb{Q}$ 上线性空间 V_n 这个代数结构的"对称群".

($\mathbb{R}$ 上 n 维欧氏线性空间 V_n 的正交线性变换的全体,线性变换的合成运算)是一个群,这里正交线性变换 ϕ 是既保持线性空间的代数结构(运算),又保持内积,即 $(\phi x, \phi y) = (x, y)$ 的变换. 这个群可看作是欧氏线性空间 V_n, 即线性空间加上一个正定内积 (x, y) 这个代数结构的"对称群".

现在来研究一下群的几条公理. G1)是多余的,因为既已知 · 是集 G 的一个运算,当然任二元素的运算结果仍在 G 中. 放在这里只是再强调一下 G 关于 · 是封闭的. 虽是多余,但实用上验证某个具体集合关于某个具体运算是否作成一个群,记住 G1)是必要的. G2)是运算的结合律. 用一下数学归纳法可证明,任意 n 个元素连乘时无论怎样加括号其运算结果总是相同的. G3)是说在 G 中存在一个元素 e 具有那里的性质,但没有说它是否是唯一的.

命题 1.4 群 $(G, \cdot)$ 中存在唯一的元素 e, 有性质:对任意 $a \in G$, 有 $ea = ae = a$.

证明 依 G3)，G 中至少有一个这样的元素.如果有两个元素 e,e' 都有这样的性质，那么 $e = ee' = e'$，即它们相等.□

我们称这个唯一的元素 e 为 G 的恒等元.

同样，我们有

命题 1.5 群 $(G,\cdot)$ 中对任意给定 $a \in G$，存在唯一的元素 b，使得 $a\cdot b = b\cdot a = e$.

证明 存在性由 G4)保证.若有两个元素 b,b' 使得

$$a\cdot b = b\cdot a = e,\ a\cdot b' = b'\cdot a = e,$$

则

$$b\cdot a\cdot b' = (b\cdot a)\cdot b' = e\cdot b' = b',$$
$$b\cdot a\cdot b' = b\cdot(a\cdot b') = b\cdot e = b,$$

故有 $b = b'$. □

我们把这个唯一元素 b 称为 a 的逆元，并记作 a^{-1}（这只是一个符号，其意义是 $a\cdot a^{-1} = a^{-1}\cdot a = e$）.我们有 $(ab)^{-1} = b^{-1}a^{-1}$，这是因为 $(ab)(b^{-1}a^{-1}) = e = (b^{-1}a^{-1})(ab)$.

群 G 中每一元 a 都有逆元 a^{-1}，这很重要.例如，利用它我们可有消去律：在群 G 中，若有 $ab = ac$（或 $ba = ca$）则必有 $b = c$.证此，只需用 a^{-1} 左乘（或右乘）两侧即得.

群的灵魂是群的运算.如果说集合是一盘散沙，则具有性质 G2)，G3)，G4)的运算·就把集合 G 非常好地组织起来.谈论关于群的问题时，一定要突出这个运算，都要和这个运算和谐.

在集合论中，两个等势的集合 M 和 N（即 M 和 N 间有一个一一对应）可以认为是"一样"的.在群论中，把两个群 $(G,\cdot)$ 和 $(H,\times)$ 看成是"一样"的，如果只知道集 G 和集 H 之间有一个一一对应 ϕ，那是完全不够的，必须要问这个对应 ϕ 和两个群的运算有什么关系.说得绝对一点，和运算没有关系的对应 ϕ 不该是我们群论中讨论的.下面的定义刻画了什么时候两个群在群论中可以看成"一样".

定义 1.6 设 $(G,\cdot)$ 和 $(H,\times)$ 是两个群，ϕ 是集 G 到集 H 上的一个一一对应.如果对任意 $x,y \in G$ 有

$$\phi(x\cdot y) = \phi(x)\times\phi(y),$$

则称 ϕ 是群 $(G,\cdot)$ 到 $(H,\times)$ 的一个同构对应.此时称群 $(G,\cdot)$ 同构于群 $(H,\times)$，记作 $(G,\cdot)\cong(H,\times)$.

请读者证明(作为练习)，如果 ϕ 是群 $(G,\cdot)$ 到群 $(H,\times)$ 的一个同构对

应，则逆映射 ϕ^{-1} 必是群 $(H,\times)$ 到群 $(G,\cdot)$ 的一个同构对应，因而如果 $(G,\cdot)\cong(H,\times)$，必也有 $(H,\times)\cong(G,\cdot)$；另外，如果 ψ 是群 $(H,\times)$ 到群 $(L,\circ)$ 的一个同构对应，则映射的合成 $\psi\circ\phi$ 是群 $(G,\cdot)$ 到群 $(L,\circ)$ 的一个同构对应，因而如果还有 $(H,\times)\cong(L,\circ)$，必也有 $(G,\cdot)\cong(L,\circ)$.

例 1.7 设 $(\mathbb{R},+)$ 是全体实数关于数的加法作成的群，而 $(\mathbb{R}^+,\cdot)$ 是全体正实数关于数的乘法作成的群. 令

$$\begin{aligned}\phi:\ \mathbb{R}^+ &\longrightarrow \mathbb{R}\\ x &\longmapsto \lg x,\end{aligned}$$

可以证明 ϕ 是此两群的一个同构对应.

利用这个同构对应可把数的乘法运算化归为数的加法运算.

定义 1.8 称群 $(G,\cdot)$ 到自身的同构对应为群 $(G,\cdot)$ 的自同构对应，简称为自同构. 群 $(G,\cdot)$ 的自同构的全体记作 Aut(G).

容易证明($\mathrm{Aut}(G)$, 变换的合成运算$\circ$)是一个群. 和在第一章 §2 中关于数域 F 的自同构群 $\mathrm{Aut}(F)$ 一样，可把这个群看作是群 $(G,\cdot)$ 这个代数结构的对称群，它刻画了群 $(G,\cdot)$ 的对称性，因而对给定群 G 计算或研究 $(\mathrm{Aut}(G),\circ)$ 这个群是群论中重要问题之一.

定义 1.9 设 $(G,\cdot)$ 和 $(H,\times)$ 是两个群，ϕ 是集 G 到 H 上的一个一一对应，如果对任意 $x,y\in G$ 有

$$\phi(x\cdot y)=\phi(y)\times\phi(x),$$

则称 ϕ 是群 $(G,\cdot)$ 到群 $(H,\times)$ 的一个反同构对应. 此时称群 $(G,\cdot)$ 反同构于群 $(H,\times)$，记作 $(G,\cdot)\cong^{-1}(H,\times)$.

同样可以证明：若 $(G,\cdot)\cong^{-1}(H,\times)$，则也有 $(H,\times)\cong^{-1}(G,\cdot)$.

彼此反同构的群，虽不能说它们完全“一样”，但基本上是一样的. 掌握其中一个群的情况，则与之反同构的那个群的情况也就清楚了.

这里我们顺便把一个符号问题交代一下. 如果 ϕ 是 M 到自身的一个映射，$x\in M$，是用 $\phi(x)$ 还是用 $x\phi$ 来表示 x 在 ϕ 下的象？只涉及一个 ϕ 时，这当然没有区别，但当用到 M 到 M 的两个映射 ϕ,ψ 的乘积 $\phi\psi$ 时，就有区别了：

用 $\phi(x)$ 时，$(\phi\psi)(x)=\phi(\psi(x))$（先 ψ 后 ϕ），

而用 $x\phi$ 时，$x(\phi\psi)=(x\phi)\psi$（先 ϕ 后 ψ）.

例如令 $M=\{1,2,3\}$ 取 $\phi=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$, $\psi=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$，则有

$$\phi\psi(1)=\phi(\psi(1))=\phi(3)=1,$$
$$1(\phi\psi)=(1\phi)\psi=2\psi=2.$$

同一个 $\phi\psi$ 在两种不同表示法下表示不同的映射.

我们再看一下下面的例子.

例 1 取群($GL_n(\mathbb{Q})$, 矩阵乘法)及群($Tr_n(V)$, 线性变换的乘法),其中 V 是 $\mathbb{Q}$ 上 n 维线性空间, $Tr_n(V)$ 是 V 的非退化线性变换全体,取定 V 的一个基: $v_1,\cdots,v_n$, 而令

$$\begin{aligned}\theta: GL_n(\mathbb{Q}) &\longrightarrow Tr_n(V)\\ A &\longmapsto T_A,\end{aligned}$$

其中

$$T_A: \quad V \longrightarrow V$$

$$x=(a_1,\cdots,a_n)\begin{pmatrix}v_1\\ \vdots\\ v_n\end{pmatrix} \longmapsto (a_1,\cdots,a_n)A\begin{pmatrix}v_1\\ \vdots\\ v_n\end{pmatrix},$$

由线性代数知 θ 是 $GL_n(\mathbb{Q})$ 到 $Tr_n(V)$ 上的一一对应.

a) 把 x 在 ϕ 下的象记作 $\phi(x)$, 此时有

$$T_A(x)=T_A\left((a_1,\cdots,a_n)\begin{pmatrix}v_1\\ \vdots\\ v_n\end{pmatrix}\right)=(a_1,\cdots,a_n)A\begin{pmatrix}v_1\\ \vdots\\ v_n\end{pmatrix},$$

这样

$$\begin{aligned}(T_BT_A)(x)=T_B(T_A(x))&=T_B\left((a_1,\cdots,a_n)A\begin{pmatrix}v_1\\ \vdots\\ v_n\end{pmatrix}\right)\\ &=(a_1,\cdots,a_n)AB\begin{pmatrix}v_1\\ \vdots\\ v_n\end{pmatrix},\end{aligned}$$

而 $T_{AB}(x)=(a_1,\cdots,a_n)AB\begin{pmatrix}v_1\\ \vdots\\ v_n\end{pmatrix}$. 故

$$\theta(AB)=T_{AB}=T_BT_A=\theta(B)\cdot\theta(A).$$

这就是说 θ 是群 $GL_n(\mathbb{Q})$ 到群 $Tr_n(V)$ 上的一个反同构对应.

b) 把 x 在 ϕ 下的象记作 $x\phi$, 此时有

$$xT_A=(a_1,\cdots,a_n)A\begin{pmatrix}v_1\\ \vdots\\ v_n\end{pmatrix},$$

这样,

$$x(T_AT_B)=(xT_A)T_B=\left((a_1,\cdots,a_n)A\begin{pmatrix}v_1\\ \vdots\\ v_n\end{pmatrix}\right)T_B$$
$$=(a_1,\cdots,a_n)AB\begin{pmatrix}v_1\\ \vdots\\ v_n\end{pmatrix},$$

而 $xT_{AB}=(a_1,\cdots,a_n)AB\begin{pmatrix}v_1\\ \vdots\\ v_n\end{pmatrix}$. 故此时

$$\theta(AB)=T_{AB}=T_AT_B=\theta(A)\theta(B),$$

这就是说 θ 是群 $GL_n(\mathbb{Q})$ 到群 $Tr_n(V)$ 上的一个同构对应.

从上面的例子看到,对映射的象用不同的表示法对问题的讨论确有影响,然而影响又确实无关紧要:只是把同构对应变成反同构对应而已.因而今后为了方便(常是因为更偏爱“同构对应”的缘故而选用 $x\phi$)我们可以任选一种,只是注意,在同一个问题中只能固定采取一种.

练习

1. 设 $(G,\cdot)$ 是群.证明:$(G,\cdot)$ 满足消去律,即对任意 $a,b,c\in G$, 若 $a\cdot b=a\cdot c$ 或 $b\cdot a=c\cdot a$, 则 $b=c$.

2. 设 $(S,\cdot)$ 是半群.对 $a\in S$, 记 $a\cdot S=\{a\cdot s\mid s\in S\}$ 和 $S\cdot a=\{s\cdot a\mid a\in S\}$.

   1) 证明:如果对任意 $a\in S$, 有 $a\cdot S=S$ 和 $S\cdot a=S$, 那么 $(S,\cdot)$ 是群.

   2) 证明:如果 $(S,\cdot)$ 是有限半群(即 S 的元素个数有限)且满足消去律,那么对任意 $a\in S$, 有 $a\cdot S=S$ 和 $S\cdot a=S$. 特别地, $(S,\cdot)$ 是群.

3. 设 ϕ 是群 $(G,\cdot)$ 到群 $(H,\times)$ 的一个同构对应.证明逆映射 ϕ^{-1} 是群 $(H,\times)$ 到群 $(G,\cdot)$ 的同构对应.

4. 设 $(\mathbf{Z},+)$ 是通常的整数加群.在 $\mathbf{Z}$ 上定义一个新的运算 $\oplus$ 如下:对任意 $a,b\in\mathbf{Z}$, 规定 $a\oplus b=a+b-1$. 证明:

   1) $(\mathbf{Z},\oplus)$ 是一个交换群.

   2) $$\phi:\ (\mathbf{Z},+)\longrightarrow(\mathbf{Z},\oplus),\quad a\longmapsto a+1$$

   是群同构对应.

§2 子群

对于这个新的数学对象——群,应该如何入手,从哪几个方面去研究它,是读者急于想了解的事.我们曾经研究过其他代数对象,如数、多项式、矩阵等,但这些似乎和群的味道不太一样.当然,在群自然出现的那些地方,如图形

的对称群、一元多项式根的对称群——Galois 群，应该对群的进一步研究提出些问题来．概括些说，对群的研究可分为互相联系的两大块：群的结构和群的表示．

事物都有其结构，但如何研究例如社会的结构，或交响乐的结构，又是很难一下子说清的．群的结构也是这样．但有些问题是可以研究的，如：§1 末提到的研究群的对称性可看作是群的结构研究中的一个问题；对群进行分类，把属于某些特别群类中的群都清楚地给出来，这是群的结构的中心问题；给定一个群，尽可能多地了解群的运算是如何把它组织起来的，等等．群和集合比较起来就是多一个运算，所以群论的初步可以仿照集合论去讨论．只是记住关于群的一切讨论都要围绕这个运算进行．

以下将群 $(G,\cdot)$ 简记为群 G．其恒等元是 e，其运算 $\cdot$ 称作乘法，常将 $a\cdot b$ 写成 ab．先看群 G 中的一个元素 a 和运算的联系，这当然首先是若干个 a 相乘．记 $a^0=e$，a^{-1} 是 a 的逆元．对任意正整数 n，归纳地定义 $a^{n+1}=(a^n)\cdot a$ 和 $a^{-(n+1)}=a^{-n}\cdot a^{-1}$．这样对任意整数 m，a^m 都有了定义．和数的幂类似，用一下数学归纳法可证得：对任意 $n,m\in\mathbf{Z}$，有 $a^n\cdot a^m=a^{n+m}$．对于交换群我们常把其运算记成 $+$，其恒等元记作 0．这时 n 个 a 相加则记为 na，此时相应的式子就变成 $na+ma=(n+m)a$．

定义 2.1 设 $a\in G$．若有正整数 n，使得 $a^n=e$ 而对任意小于 n 的正整数 m，$a^m\neq e$，则称 a 的阶为 n；否则，即对任意正整数 n 都有 $a^n\neq e$，则规定 a 的阶为 ∞．

依定义，e 的阶是 1．

群 G 的运算一般是不交换的，即 ab 不一定等于 ba．因而群中与其它元素可交换的元素占据特殊的地位．

定义 2.2 设 $a\in G$．若对任意 $x\in G$，有 $ax=xa$，则称 a 为群 G 的中心元．

容易证明，若 a 是中心元，则 a^{-1} 也是中心元；另外 e 是中心元．

再看群 G 的子集 H 和运算的联系，为此自然要引入下面集合．对 G 的任意两个子集 H,K 规定：

$$H\cdot K=\{xy\mid x\in H,y\in K\},$$
$$H^{-1}=\{x^{-1}\mid x\in H\}.$$

如果说在集合论中对集合的子集都一视同仁，那么在群论中却不是这样，我们对那些与运算关系不好的子集不太喜欢，而由于运算的关系，对满足

$H \cdot H \subseteq H, H^{-1} \subseteq H$ 的子集 H 给以突出的地位.

定义 2.3 设 H 是群 G 的非空子集.若有

S1) $H \cdot H \subseteq H$, 即对任意 $a, b \in H$, 有 $ab \in H$;

S2) $H^{-1} \subseteq H$, 即对任意 $a \in H$, 有 $a^{-1} \in H$;

我们则称 H 为群 G 的子群.

一个群 G 至少有两个子群: G 和 $\{e\}$, 称之为平凡子群.不同于 G 的子群,称为 G 的真子群.

子群是非常重要的概念,群论中感兴趣的群的子集都是和子群密切联系的,或者简直就是由子群导出的那些子集.了解子群的情况,是了解群的结构的一个重要方面,一个具有很多子群的群,其结构也会复杂一些.

命题 2.4 设 H 是 G 的子群,则

1) G 的运算 · 也是 H 的运算,仍记作 ·.

2) $(H, \cdot)$ 是一个群, $e \in H$.

证明 1) 由于 $H \cdot H \subseteq H$, 当然 · 是 H 的一个运算.

2) 运算 · 在 G 中满足结合律,当然在 H 中也满足结合律,因此有 G2). 任取 $a \in H$(因为 H 非空),则由 S2),有 $a^{-1} \in H$, 又由 S1)知 $e \in H$. 当然 e 在 H 中也是恒等元,即得 G3).注意到 $H^{-1} \subseteq H$, 则 G4)也是成立的.□

这样,子群 H 就是在群 G 的运算下自身也是群的那些子集.

子群的交和并还是子群吗? 群 G 的两个子群 H_1, H_2 的并一般不再是子群,例如取 $h_1 \in H_1 \setminus H_2, h_2 \in H_2 \setminus H_1$, 则有 $h_1 h_2 \notin H_1 \cup H_2$. 这是因为若 $h_1 h_2 = h \in H_1$, 则用 h_1^{-1} 从左乘 $h_1 h_2 = h$ 的两侧,便得 $h_2 = h_1^{-1} h \in H_1$, 而这是和 h_2 的取法矛盾的.同样可证 $h_1 h_2 \notin H_2$.

命题 2.5 设 $H_i, i \in I$(一个有限或无限的指标集),都是群 G 的子群,则 $H = \bigcap_{i \in I} H_i$ 也是群 G 的子群.

证明 因为对任意 $i \in I$, 有 $e \in H_i$, 故 H 不会是空集.任取 $a, b \in H$, 则对任意 $i \in I$, 有 $a, b \in H_i$. 因为每个 H_i 是子群,故 ab, a^{-1} 都在 H_i 中,即 $ab, a^{-1} \in H$. 故 H 是一个子群.□

任取群 G 中的一个子集 M, 我们问是否有一个包含 M 的最小子群 H, 即有 1) $M \subseteq H$, 2) 若 $M \subseteq H'$ 而 H' 也是子群,则有 $H \subseteq H'$. 如果含 M 的最小子群 H 存在,则它必是唯一的,这是因为,若 H_1, H_2 是含 M 的最小子群,由条件 2)知 $H_1 \subseteq H_2, H_2 \subseteq H_1$, 故有 $H_1 = H_2$. 它的存在性可由下面命

题得到.

命题 2.6 M 是群 G 的子集,设 $H_i, i \in I$, 是群 G 中含 M 的所有子群. 则 $H = \bigcap_{i \in I} H_i$ 是含 M 的最小子群.

证明 首先 G 是含 M 的子群,因而 I 不是空集. 依上一命题 H 是子群. 显然 $M \subseteq H$. 若 $M \subseteq H'$ 且 H' 是子群,则 H' 是 H_i 中的某一个,故有 $H = \bigcap_{i \in I} H_i \subseteq H'$. □

此命题只是肯定含 M 的最小子群 H 的存在性,然而不是构造性的,即对 H 是由什么样的元素组成,没有什么了解. 下面我们独立于命题 2.6,从构造的观点,找出含 M 的最小子群 H.

如果 M 是子群,即有 $M \cdot M \subseteq M, M^{-1} \subseteq M$, 显然此时 $H = M$. 如果 M 是空集,显然 $\{e\}$ 是含 M 的最小子群. 如果 M 非空但不是子群,那么存在 $a, b \in M$, 使得 $ab \notin M$ 或 $a^{-1} \notin M$, 这时我们把这些元素都添加到 M 上去,即令

$$H = \{x_1 x_2 \cdots x_n \mid n \text{ 是自然数}, x_i \in M \cup M^{-1}\}, \tag{1}$$

用话来说,这就是考虑由 M 的元素和 M^{-1} 的元素,以及由 M 及 M^{-1} 中取出任意 n 个元素作乘积所得到的元素全体. 容易证明 $H \cdot H \subseteq H, H^{-1} \subseteq H$, 即 H 是含 M 的子群. 另一方面,若有子群 $K \supseteq M$, 则 $K \supseteq M^{-1}$, 令 $M' = M \cup M^{-1}$, 即有 $K \supseteq M'$. 这样 K 必包含 $M' \cdot M'$, 随之必包含 $(M' \cdot M') \cdot M', \cdots$, 故知 $K \supseteq H$. 即证得 H 是含 M 的最小子群.

定义 2.7 1) 群 G 中含 M 的最小子群称为 M 在 G 中生成的子群,记作 $\langle M \rangle$.

2) 设 H 是群 G 的一个子群. 如果子集 $M \subseteq H$ 且 $\langle M \rangle = H$, 则称 M 是子群 H 的一个生成元集.

3) 特别,当 $M \subseteq G$ 而 $\langle M \rangle = G$ 时,称 M 生成群 G, 而 M 是群 G 的一个生成元集.

在下一节中我们将进一步讨论生成元集.

在本节的最后,我们再一次回到"对称"问题. 如果把群 G 比作平面(这时该把运算比作距离),而把子群比作图形(为什么我们只把子群而不把子集比作图形呢?),则自然可以谈论子群的对称.

命题 2.8 1) 群 G 的中心元的全体 C 是一个子群;称之为群的中心.

2) 子群 C 在群 G 的任意自同构 ϕ 下是不变的: $\phi C \subseteq C$.

证明 1)是显然的,而 2)可以很容易地证明如下:任取 $c \in C$ 和 $x \in G$

有 $cx = xc$，随之 $\phi(c)\cdot\phi(x) = \phi(x)\cdot\phi(c)$. 但由于 ϕ 是 G 到 G 上的一一对应，故 $\phi(x)$ 可为 G 中任意元，即 $\phi(c)$ 可和 G 中任意元交换，故 $\phi(c)\in C$. □

这样，群的中心是一个"绝对对称"的子群.

给了群 G，一般不太容易计算出群 $\mathrm{Aut}(G)$. 但我们却很容易找到它的一个子群.

任取 $a\in G$，命

$$T_a:\ G \longrightarrow G$$
$$x \longmapsto axa^{-1}.$$

直接验证可知 T_a 是 G 到 G 上的一个一一对应. 由

$$T_a(xy) = a(xy)a^{-1} = (axa^{-1})(aya^{-1}) = T_a(x)\cdot T_a(y),$$

还知 T_a 保持运算，这样 $T_a\in\mathrm{Aut}(G)$. 易见 $T_e = I$（恒等自同构），当然我们还知道对中心 C 中的任意元 c，有 $T_c = I$.

令 $\mathrm{Inn}(G) = \{T_a | a\in G\}$，则由

$$(T_aT_b)(x) = T_a(T_b(x)) = T_a(bxb^{-1}) = a(bxb^{-1})a^{-1}$$
$$= (ab)x(b^{-1}a^{-1}) = (ab)x(ab)^{-1} = T_{ab}(x),\quad \forall\ x\in G,$$

知 $T_aT_b = T_{ab}$. 由此又知 $T_aT_{a^{-1}} = T_{a^{-1}}T_a = T_e$，即 $(T_a)^{-1} = T_{a^{-1}}$，故 $\mathrm{Inn}(G)$ 关于乘法和取逆元是封闭的，即它是 $\mathrm{Aut}(G)$ 的一个子群.

定义 2.9 1) 称 T_a 为群 G 的内自同构对应，而称 $\mathrm{Inn}(G)$ 为群 G 的内自同构群；

2) 如果 G 的一个子群 H 在内自同构群 $\mathrm{Inn}(G)$ 的作用下不变，即指对任意 $T_a, a\in G$，都有 $T_a(H)\subseteq H$，则称 H 为 G 的正规子群(或不变子群).

凡是重要的东西都会有一定的对称性，对称性好的东西也常会发挥一定好作用. 正规子群，在 $\mathrm{Aut}(G)$ 的子群 $\mathrm{Inn}(G)$ 作用下不变，因而具有一定的对称性，可以期望它在所有子群中有一些特殊作用.

由于群的运算有结合律，故对群 G 的三个子集 M, N, P 而言，也有 $(M\cdot N)\cdot P = M\cdot(N\cdot P)$，因而可把它们和元素的乘积一样简单地写成 $M\cdot N\cdot P$ 而不必加括号. 注意到这一点，对 G 的正规子群 H 我们有

$$\forall\ a\in G,\quad T_a(H) = aHa^{-1}\subseteq H,$$

包含号的两边从右侧用 a 去乘，得 $\forall\ a\in G, aH\subseteq Ha$，特别对 $a^{-1}\in G$，也有 $a^{-1}H\subseteq Ha^{-1}$，故 $a(a^{-1}H)a\subseteq a(Ha^{-1})a$，即 $Ha\subseteq aH$. 这样便有

$$\forall\ a\in G,\quad aH = Ha. \tag{2}$$

(2)并不是说，H 中的元素 h 和 a 相乘时可交换，即有 $ah = ha$，而是说"集体"可交换，即对任一 $h \in H$，必有 $h' \in H$ 使得 $ah = h'a$，也有 $h'' \in H$ 使得 $ha = ah''$. (2)也蕴含着

$$\forall\ M \subseteq G,\quad M \cdot H = H \cdot M. \tag{3}$$

(3)可以看作正规子群 H 的定义，即子群 H 是正规子群当且仅当 H 和 G 的任意子集 M 相乘时可交换. 这样正规子群在 G 的所有子集中的地位有点类似中心元在 G 的所有元素中的地位.

对于交换群来说，当然每一个元素都是中心元，每一子群都是正规子群.

练习

1. 设群 G 中元素 a 的阶为 $n(< \infty)$. 证明：对任意正整数 m，若 $a^m = e$，则 $n \mid m$.
2. 设 a, b 是群 G 中的两个元. 证明：ab 与 ba 有相同的阶.
3. 设 H 和 K 是群 G 的两个子群. 证明：
   1) HK 是 G 的子群当且仅当 $HK = KH$；
   2) 当 H 是 G 的正规子群时，HK 是 G 的子群.
4. 找出对称群 S_3 的所有子群和正规子群.
5. 设 G 是群. 证明：内自同构群 $\mathrm{Inn}(G)$ 是自同构群 $\mathrm{Aut}(G)$ 的正规子群.

§3 生成元集，循环群

研究一个对象可粗分为两种方法：一种方法是研究此对象的内部关系，另一种是把此对象放在与其它对象的相互联系中去研究. 当我们对一个群"孤立地"去研究时，掌握这个群的一个好的生成元集常是非常有帮助的.

现在给出一些具体群的生成元集.

例 1 设 G 为平面的所有运动组成的群. 在平面内取定一笛卡尔坐标系，这样在此平面上我们有一个特定点——原点，和一个特定直线—— x - 轴. 在平面的运动中选取下列特定运动，并表以特定符号：t_a：沿向量 a 的平移；ρ_θ：绕原点转(逆时针方向) θ 角的旋转；r：关于 x - 轴的翻摺. 如果用坐标表示，记 $x = (x_1, x_2)^T$，则有

$$t_a(x) = x + a = \begin{pmatrix} x_1 + a_1 \\ x_2 + a_2 \end{pmatrix},$$

$$\rho_\theta(x) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix},$$

$$r(x)=\begin{pmatrix}x_1\\-x_2\end{pmatrix}=\begin{pmatrix}1&0\\0&-1\end{pmatrix}\begin{pmatrix}x_1\\x_2\end{pmatrix}.$$

显然 t_a,ρ_θ,r 只是一部分运动,例如绕其他点(非原点)的旋转和关于 y - 轴的翻摺都不在其中.然而很容易证明 $\{t_a(\forall a),\rho_\theta(\forall\theta),r\}$ 是群 G 的一个生成元集,这是因为任一运动 t 可写成

$$t(x)=\begin{pmatrix}a_{11}&a_{12}\\a_{21}&a_{22}\end{pmatrix}\begin{pmatrix}x_1\\x_2\end{pmatrix}+\begin{pmatrix}a_1\\a_2\end{pmatrix},$$

其中 2 阶矩阵,记作 A,是正交矩阵.由线性代数知

$$A=\begin{pmatrix}\cos\theta&-\sin\theta\\\sin\theta&\cos\theta\end{pmatrix},\text{若 }A\text{ 的行列式}|A|=1.$$

$$A=\begin{pmatrix}\cos\theta&-\sin\theta\\\sin\theta&\cos\theta\end{pmatrix}\begin{pmatrix}1&0\\0&-1\end{pmatrix},\text{若}|A|=-1.$$

故

$$t(x)=t_a\rho_\theta(x)\quad\text{或}\quad t(x)=t_a\rho_\theta r(x).\tag{1}$$

回到非坐标形式,即有 $t=t_a\rho_\theta$ 或 $t=t_a\rho_\theta r$,亦即任一运动都能表示成 t_a,ρ_θ,r 的乘积.这即证得 $\{t_a(\forall a),\rho_\theta(\forall\theta),r\}$ 是群 G 的一个生成元集.

一般而言,用生成元去表示群中元素时,表示法不是唯一的.但在我们这个情形中 t 在(1)中的表示还是唯一的:若 $t_a\rho_\theta=t_b\rho_\eta$,则必有 $a=b,\theta=\eta$ 且 $t_a\rho_\theta$ 永远不会写成 $t_b\rho_\eta r$ 的形状.

如果还能知道生成元之间的运算规则,则我们不仅可以用它们表示群中任一元素,还能利用这些规则去计算群中任意两个元素的乘积.无论是用平面几何方法或者线性代数方法,都容易验证(留给读者)下列规则:

$t_at_b=t_{a+b},\quad \rho_\theta\rho_\eta=\rho_{\theta+\eta},\quad r^2=e$ (恒等运动)

$\rho_\theta t_a=t_{a'}\rho_\theta$,其中 $a'=\rho_\theta(a)$.

$rt_a=t_{a'}r$,其中 $a'=r(a)$.

$r\rho_\theta=\rho_{-\theta}r$.

以上是否是生成元间的所有关系,这是目前我们无法说清的.无论如何,在讲自由群时,我们将给出一个判断标准,由之可以知道,这些关系就是所有的或不是所有而有漏掉的.

利用这些规则我们可将两个表成标准形式(1)的元素的乘积写成标准形

式(1).

例 2 找出 n 元对称群 S_n 的生成元集.

首先明确一下,今后谈及群 S_n 时,两个置换的乘积是自左向右的,例如

$$\begin{pmatrix}1 & 2 & 3 & \cdots & n\\ 2 & 4 & 7 & \cdots & \cdots\end{pmatrix}\begin{pmatrix}1 & 2 & \cdots\\ 3 & 5 & \cdots\end{pmatrix}=\begin{pmatrix}1 & \cdots\\ 5 & \cdots\end{pmatrix}.$$

我们称一个置换 π 是 t - 循环置换,或 t - 轮换,如果 $i_1\pi = i_2, i_2\pi = i_3, \cdots, i_{t-1}\pi = i_t, i_t\pi = i_1$ 且 $i\pi = i, i \notin \{i_1, i_2, \cdots, i_t\}$. 此时把 π 简记作: $\pi = (i_1 i_2 \cdots i_t) = (i_2\, i_3 \cdots i_t\, i_1)$, 这是因为在一个有方向轮换中,先后相邻位置是主要的,谁起头是无关紧要的.如果 $\{i_1, \cdots, i_t\}$, $\{j_1, \cdots, j_s\}$ 不相交,易见相应的循环置换可交换,即

$$(i_1 \cdots i_t)(j_1 \cdots j_s) = (j_1 \cdots j_s)(i_1 \cdots i_t).$$

取任一置换 π, 从 n 个数中任取一个数 i_1, 然后用 π 不断地去作用: $i_1\pi = i_2, i_2\pi = i_3, \cdots$, 由于只有 n 个数,故总会有 $i_t\pi = i_1$, 即回到最初的那个数 i_1, 这样得到一个在 π 作用下的循环小组 $\{i_1, i_2, \cdots, i_t\}$. 再从此循环小组以外取一数 j_1, 如上去作,得在 π 作用下的另一循环小组 $\{j_1, j_2, \cdots, j_s\}$. 由于 π 是集 $\{1, \cdots, n\}$ 的一个一一对应,故在前面循环小组中出现的数不会在后面的循环小组中再出现,亦即所有可能得到的这些循环小组之间两两不相交且其并集便是 $\{1, \cdots, n\}$. 此时易见, π 可表为一些不相交的轮换的乘积,即

$$\pi = (i_1\, i_2 \cdots i_t)(j_1\, j_2 \cdots j_s)\cdots(k_1\, k_2 \cdots k_r).$$

至此,我们可以说,所有轮换组成 S_n 的一个生成元集.

对轮换进一步分解,我们有

$$(i_1 \quad i_2 \quad \cdots \quad i_t) = (i_1 \quad i_2)(i_1 \quad i_3)\cdots(i_1 \quad i_t),$$

即每一 t - 轮换可分解成 2 - 轮换(特称之为对换)的乘积.这样所有对换 $(i \quad j), i, j \in \{1, \cdots, n\}$, 组成 S_n 的另一个生成元集.(对于它,在定义行列式时似曾相识!)希望生成元集小是我们选生成元集的一个标准,因而这个生成元集比上一个好.

进一步的计算(留给读者)可知 $\{(1 \quad 2), (2 \quad 3), \cdots, (n-1 \quad n)\}$ 足够用了,它也是 S_n 的一个生成元集.若令 $T_i = (i \quad i+1), i = 1, 2, \cdots, n-1$, 则简单计算可知它们之间有下列关系:

$$T_1^2 = T_2^2 = \cdots = T_{n-1}^2 = e,$$

$$(T_iT_{i+1})^3 = e \quad (1 \leqslant i \leqslant n-2),$$

$$(T_iT_k)^2 = e \quad (i \leqslant k-2).$$

希望选定的生成元之间有尽可能完全、尽可能简单的关系是我们选生成元集的另一个标准.

从以后的讨论中你会看到，在一个有限群中找到一个真正规子群是一个很有益的事.现在我们对群 S_n 作这件事.

令所有以有理数作系数的变元 $x_1,\cdots,x_n$ 的多项式全体为 $P=\mathbb{Q}[x_1,\cdots,x_n]$. 利用 $\pi\in S_n$，可如下定义 P 到 P 的一个映射(仍记作 π)：对任意 $f(x_1,\cdots,x_n)\in P$ 规定

$$f(x_1,\cdots,x_n)\pi=f(x_{1\pi},\cdots,x_{n\pi}),\tag{2}$$

例如 $f(x_1,\cdots,x_n)e=f(x_1,\cdots,x_n)$， e 是 S_n 的恒等元.

$(x_1x_2+x_1x_2x_3)(1\ \ 4\ \ 2\ \ 8\ \ 3)=x_4x_8+x_4x_8x_1$.

(2)说明我们是把群 S_n 中的元素 π 从右侧作用到 P 中元素，这和 π 也是从右侧作用到 $\{1,2,\cdots,n\}$ 上是相协调的.注意到这一点，就知

$$(f(x_1,\cdots,x_n)\pi)\sigma=f(x_1,\cdots,x_n)(\pi\sigma),\quad \pi,\sigma\in S_n.\tag{3}$$

令

$$t(x_1,\cdots,x_n)=\prod_{i=1}^{n-1}(x_i-x_{i+1})(x_i-x_{i+2})\cdots(x_i-x_n).$$

显然对任意 $\sigma\in S_n$，$t(x_1,\cdots,x_n)\sigma=t(x_1,\cdots,x_n)$ 或 $t(x_1,\cdots,x_n)\sigma=-t(x_1,\cdots,x_n)$. 若出现第一种情形，称 σ 为偶置换，若是第二种情形，则称 σ 为奇置换.若 π,σ 是偶置换，由(3)的左侧可知先用 π 作用 t 不变，再用 σ 作用 t 还是不变，而从(3)的右侧便得乘积 $\pi\sigma$ 作用 t 后 t 不变，故 $\pi\sigma$ 是偶置换，即偶置换之积仍是偶置换.

令 A_n 表示 S_n 中一切偶置换的全体.易知 A_n 是 S_n 的子群，并且还是正规子群.(证明!)称群 A_n 为 n 元交代群.

例 3 找出群 A_n 的一个生成元集.

由于对换是奇置换，故 A_n 中的元素必可表成偶数个对换的乘积.两个对换若含共同数，这时我们有，例如 $(1\ \ 2)(1\ \ 3)=(1\ \ 2\ \ 3)$；若不含共同数，则有，例如 $(1\ \ 2)(3\ \ 4)=(1\ \ 2)(2\ \ 3)(2\ \ 3)(1\ \ 4)=(1\ \ 2\ \ 3)(3\ \ 2\ \ 4)$. 即两个对换乘积永远可表示为二个 3－轮换的乘积.随之任一偶置换均可表成 3－轮换的乘积.3－轮换，作为两个对换的乘积，当然是偶置换.这样所有 3－轮换 $(i_1\ \ i_2\ \ i_3)$ 组成 A_n 的一个生成元集.

例 4 设 $SL_n(\mathbb{Q})$ 是有理数域 $\mathbb{Q}$ 上所有其行列式为 1 的 n 阶矩阵的全体.易见，$SL_n(\mathbb{Q})$ 关于矩阵的乘法作成一个群，称之为特殊线性群.现在来找它的一个生成元集.

设 I 是 n 阶单位矩阵，而 $E_{ij}(a)$，$i\neq j$ 是在 i 行 j 列交处为 a 而其余位置上为 0 的 n 阶矩阵.称形如 $I+E_{ij}(a)$ 的矩阵为初等矩阵，它的行列式等于 1，即在 $SL_n(\mathbb{Q})$ 中.今证：所有初等矩阵 $I+E_{ij}(a)$（$a\in\mathbb{Q},i\neq j,1\leqslant i,j\leqslant n$）组成特殊线性群 $SL_n(\mathbb{Q})$ 的一个生成元集.

由线性代数知,用这种初等矩阵右乘(或左乘)一个矩阵就等于把它的某一行(列)乘以一个数加到另一行(列)上去.利用这种初等变换很容易把一个非退化矩阵 M 变成下面形状,即有初等矩阵 T_i, E_j 使

$$T_1 T_2 \cdots T_s M E_1 E_2 \cdots E_t = \begin{pmatrix} 1 & & & 0 \\ & \ddots & & \\ & & 1 & \\ 0 & & & a \end{pmatrix},$$

但若 $M \in SL_n(\mathbb{Q})$,即它的行列式为 1,则两边取行列式便得 $a = 1$,即有

$$M = T_s^{-1} \cdots T_1^{-1} E_t^{-1} \cdots E_1^{-1}.$$

但初等矩阵之逆仍是初等矩阵,即证得初等矩阵全体是 $SL_n(\mathbb{Q})$ 的一个生成元集.

特别 $\left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} \middle| a \in \mathbb{Q} \right\}$ 是 2 阶特殊线性群 $SL_2(\mathbb{Q})$ 的一个生成元集.

有了生成元集的概念之后,我们可以划分一些群类.

定义 3.1 1) 由一个元素 a 生成的群 G,即 $\langle a \rangle = G$,称为循环群.

2) 由有限个元素生成的群 G,即 $\langle a_1, \cdots, a_n \rangle = G$,称为有限生成群.

命题 3.2 如果 G 是一个循环群,则 G 必有下列形状.

1) $G = \{\cdots, a^{-n}, \cdots, a^{-2}, a^{-1}, e, a, a^2, \cdots, a^m, \cdots\} = \{a^n \mid n \in \mathbb{Z}\}$,其中 $a^n = a^m$ 当且仅当 $n = m$;

2) $G = \{e, a, a^2, \cdots, a^{n-1}\}$,其中 $a^n = e$ 而 $a^s = a^t, 0 \leqslant s, t \leqslant n-1$,当且仅当 $s = t$.

证明 G 是循环群,故有 $G = \langle a \rangle, a \in G$.

若 a 的周期是 ∞,则对任意整数 n, m,若 $n \neq m$,必有 $a^n \neq a^m$.否则,若 $a^n = a^m$,则有 $a^{n-m} = a^n a^{-m} = a^m a^{-m} = e$,这与 a 的周期是 ∞ 相矛盾.再由 §2 中(1)式,便得命题中 1)的情形.

若 a 的周期是 n,则 $\{e, a, a^2, \cdots, a^{n-1}\}$ 由 n 个不同元素(证明!)组成且关于乘法和取逆(例如 $a^{-1} = a^{n-1}, (a^s)^{-1} = a^{n-s}$)是封闭的,即它是含 a 的子群,故有 $G = \langle a \rangle = \{e, a, \cdots, a^{n-1}\}$ 而得命题中的 2).□

这个命题说,如果存在循环群 G 的话,那么 G 一定是那种样子.但这完全不能说明,循环群确实是存在的.下面的例子说明这两种形状的循环群都存在.

例 5 ($\mathbb{Z}$,数的加法)是无限循环群.易知 $\mathbb{Z} = \langle 1 \rangle$,这是因为,在我们这种情况,命题 3.2 中的 a 相当于 1,而 a^n 相当于 $\underbrace{1+1+1+1}_{n} = n$.类似地,

a^{-n} 相当于 $-n$,这里 n 是正整数.

例 6 设 n 是正整数,考察由绕原点的旋转 $\rho_\theta, \theta = \frac{2\pi}{n}$,所生成的群 $C_n = \langle \rho_\theta \rangle = \{\rho_\theta^i \mid 0 \leqslant i \leqslant n-1\}$. 这是一个阶为 n 的循环群.

这样,我们有一个无限循环群 $(\mathbb{Z}, +)$ 和一个 n 阶循环群 C_n.

另一方面,任意取一个循环群 G,由命题 3.2,或有 $G = \{\cdots, a^{-n}, \cdots, a^{-2}, a^{-1}, e, a, a^2, \cdots, a^n, \cdots\}$,这时,直接验证知

$$\begin{aligned} \theta_1: \quad \mathbb{Z} &\longrightarrow G \\ m &\longmapsto a^m \end{aligned}$$

是群 $\mathbb{Z}$ 到群 G 的一个同构对应;或有 $G = \{e, a, \cdots, a^{n-1}\}$,这时,直接验证知

$$\begin{aligned} \theta_2: \quad C_n &\longrightarrow G \\ \rho_\theta^s &\longmapsto a^s, \quad s \in \{0, 1, 2, \cdots, n-1\} \end{aligned}$$

是群 C_n 到群 G 的一个同构对应. 如果把同构的群看成相同的,总结一下上面的讨论就有

定理 3.3 循环群有且仅有 $(\mathbb{Z}, +)$ 和 $C_n, n \in \mathbb{N}$.

这样我们就完全刻画了循环群类:列出所有可能的循环群. 我们当然希望对其它给定的群类也能达到这个目标. 但这对几乎所有的群类都是难以达到的(以后将介绍的有限生成交换群类是极少数例外之一),这是因为群的构造太复杂,而循环群类是一个太特殊的类. 原则上阶为 5000 的群当然是可以列举的,也许你能写一个程序通过计算机把它列举出来,然而这绝不是一个简单的工作.

练习

1. 设 $\tau = (i_1 i_2 \cdots i_t)$ 是一个轮换,求 τ 的逆和阶.
2. 证明:循环群 $G = \langle a \rangle$ 的任一子群也是循环群.
3. 设 a 是群 G 中阶为 n $(<\infty)$ 的元素. 对任意正整数 s,证明:

   1) a^s 的阶为 $\frac{n}{(s, n)}$,这里 (s, n) 是 s 与 n 的最大公因子;

   2) a^s 与 $a^{(s,n)}$ 有相同的阶;

   3) $\langle a^s \rangle = \langle a^{(s,n)} \rangle$.

4. 设 G 是由两个元素 a 和 b 生成的群. 已知 a 和 b 有下列关系 $a^2 = e, b^3 = e$ 和 $ab = b^2 a$. 试写出 G 中所有的元素.
5. 证明:

   1) $\{(12), (23), \cdots, ((n-1)n)\}$ 是 S_n 的一个生成元集;

   2) $\{(12), (13), \cdots, (1n)\}$ 是 S_n 的一个生成元集;

3) $\{(123),(124),\cdots,(12n)\}$ 是 A_n 的一个生成元集.

§4 子群(续)

在§2中我们一般地讨论了子群,下面作为例子我们考虑一下平面运动群的子群.找出所有子群常是不太现实的问题,而找出具有一定性质的子群类常是有趣和有意义的问题.现在我们提出问题:平面运动群的所有有限子群是哪些?这就是问,平面图形的有限对称群是些什么样的群?

命题 4.1 设 G 是平面运动群的有限子群,则平面上必有一点 p,使得对任意 $g \in G$,有 $g(p) = p$.

证明 令 $|G| = n$,在平面上任取一点 s,作点集 $A = \{g(s) \mid g \in G\}$(若有相同者,我们计重复数,即认定 A 中有 n 个元素).引入坐标后,则点集 A 的重心 p 的坐标(仍记作 p)与 $g(a), g \in G$ 的坐标间的关系是:

$$p = \frac{1}{n}\sum_{g \in G} g(s). \qquad (*)$$

任取运动 ϕ,而证 ϕ 将 n 个点的集 $\{s_1,\cdots,s_n\}$(可有重复)的重心移到变动后的点集 $\{\phi(s_1),\cdots,\phi(s_n)\}$ 的重心,即要证:若 $p = \frac{1}{n}\sum_{i=1}^{n} s_i$,则

$$\phi(p) = \frac{1}{n}\sum_{i=1}^{n}\phi(s_i). \qquad (**)$$

这从物理上看是显然的:把一个物体刚体运动到另一个地方去,重心当然也跟着过去了.再注意到,对 G 中任意元素 h,有 $hG = \{hg \mid g \in G\} = G$,将 $(**)$ 应用到 $(*)$ 便有

$$h(p) = \frac{1}{n}\sum_{g}(hg)(s) = \frac{1}{n}\sum_{g} g(s) = p, \quad \forall\ h \in G,$$

即 p 就是所求点.

如果愿意对 $(**)$ 有一个数学上的证明,则可如下去作:由前知任一运动 ϕ 总是 t_a, ρ_θ 以及 r 的一个乘积,因而欲证 $(**)$,只要对这三者去验证就行了.

若 $\phi = t_a$,则 $\phi(p) = p + a, \phi(s) = s + a$,故有 $(**)$.

若 $\phi = \rho_\theta$ 或 r,则 ϕ 是线性变换,当然 $(**)$ 也成立.□

上面证明中涉及的点集 A(常称之为点 s 在群 G 作用下的轨道)以及 $(*)$ 中的 p(物理中称之为重心,数学上叫做“平均”点)是很有用的概念.很有意思的一个现象是,在点集 $A = \{g(s) \mid g \in G\}$ 中每一点的重复度是相同的,即若点 s(它当然在集 A 中)重复出现 10 次,则 A 中任一点都重复出现

10 次. 读者可试证一下.

称满足性质对任意 $g \in G$, 有 $g(p)=p$ 的点 p 为群 G 的不动点, 上命题是说, 平面运动群的任一有限子群 G 都有不动点.

定理 4.2 设 G 是平面运动群的一个有限子群, 则适当选取坐标系, G 必是下列两种类型之一:

(a) $G=C_n$, 由绕原点的旋转 $\rho_\theta, \theta=\frac{2\pi}{n}$ 所生成的 n 阶群: $C_n=\langle \rho_\theta \rangle = \{\rho_\theta{}^i \mid 0 \leqslant i \leqslant n-1\}$.

(b) $G=D_n$, 由绕原点的旋转 $\rho_\theta, \theta=\frac{2\pi}{n}$ 及沿 x - 轴的翻摺 r 所生成的阶为 $2n$ 的二面体群: $D_n=\langle \rho_\theta, r\rangle=\{\rho_\theta{}^i, \rho_\theta{}^i r \mid 0 \leqslant i \leqslant n-1\}$.

证明 取 G 的不动点 O 作原点, 任取 $g \in G$, 由于 $g(O)=O$, 故 g 或是绕 O 点的旋转 ρ_θ, 或是沿过 O 点直线的翻摺.

(a) G 中元素都是旋转. 若 $G \neq \{e\}$, 则有 G 中有旋转 $\rho_\theta, 0<\theta<2\pi$.

由于 G 中只有有限个元素, 故 G 中必有 ρ_θ, θ 在属于 G 的旋转中为最小者. 此时对 G 中任意非平凡旋转 $\rho_\alpha, 0<\alpha<2\pi$, 将其中 α 表成 $\alpha=m\theta+\beta$, $0 \leqslant \beta<\theta$, 这时由于

$$\rho_\beta=\rho_{\alpha-m\theta}=\rho_\alpha \rho_{-m\theta}=\rho_\alpha \cdot \rho_{m\theta}{}^{-1} \in G$$

以及 θ 的选择, 可知必有 $\beta=0$, 即 $\rho_\alpha=\rho_\theta{}^m$, 亦即 $G=\langle \rho_\theta \rangle$ 是有限循环群. 设其阶为 n, 则由 $\rho_\theta{}^n=e$ 知 $n\theta=2\pi$.

(b) G 中含有翻摺. 任取 G 中一个翻摺, 适当选择 x - 轴, 可认为它是沿 x - 轴的翻摺, 即为 r. 令 H 是 G 中所有旋转(包括 e)作成的子集. 易见 H 是子群, 命其阶为 n, 由(a)知 $H=\langle \rho_\theta \rangle, \theta=\frac{2\pi}{n}$. 这样 G 至少含有 $2n$ 个元素 $G'=\{\rho_\theta{}^i, \rho_\theta{}^i r \mid 0 \leqslant i \leqslant n-1\}$. 今任取 G 中元素 g, 若 g 是旋转, 则已在 G' 中, 若 g 是翻摺, 则 g 是沿过 O 点直线 l 的翻摺, 设直线 l 与 x - 轴成 α 角, 由平面几何知识可知 $g=\rho_{2\alpha} r$. 这时

$$\rho_{2\alpha}=\rho_{2\alpha} r r=g \cdot r \in G,$$

由上知 $\rho_{2\alpha}=\rho_\theta{}^i$, 因而 $g=\rho_\theta{}^i r$, 即 $g \in G'$, 即 $G=G'$. □

这样我们找出了平面运动群的所有有限子群, 就是说, 一个平面图形对称群, 如果有限的话, 必是 C_n 或 D_n. 不难对每一个 $C_n(D_n)$ 找出一个平面图形, 它的对称群就是 $C_n(D_n)$, 例如正 n 边形的对称群是 D_n. 这些平面图形, 就代表了具有有限对称群的所有平面图形. 按着这个思路, 如果把空间运动群的所

有有限子群找出来,人们就对正多面体得到完全的分类.从这里我们感到群论的力量.

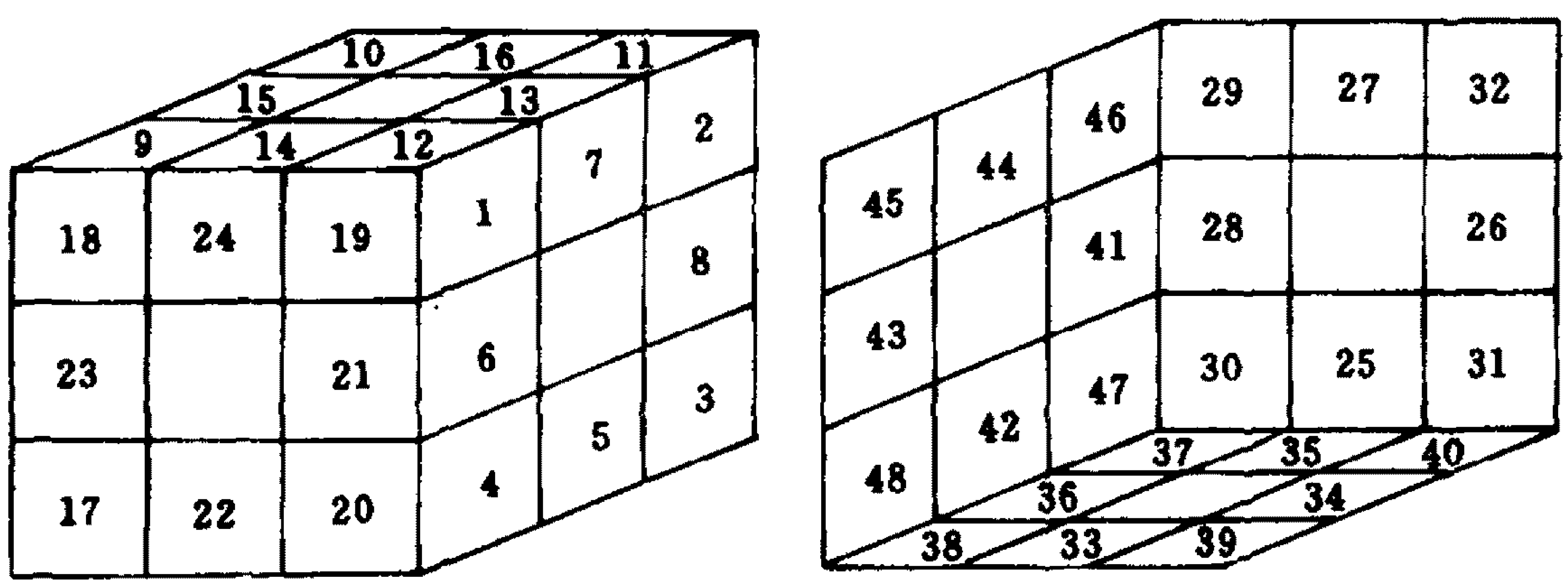
作为群的生成元集的又一个例子,这里的二面体群 $\{\rho_\theta^i, \rho_\theta^i r \mid 0 \leqslant i \leqslant n-1, \theta = \frac{2\pi}{n}\}$ 显然以 $x = \rho_\theta, y = r$ 为生成元集.由§3例1知,生成元 x, y 之间有下列关系:

$$x^n = e, \quad y^2 = e, \quad yx = x^{-1}y.$$

数学中有许多问题(计算问题,或证明问题),都可对之设计出算法,而好的算法是不难用计算机实现的.因而在我们这个计算机时代,对一类数学问题找出算法是人们非常感兴趣的事.在附录中,我们将介绍近代计算代数中的一个重要算法.在这里我们只给出一个计算例子:用MAPLE软件包计算48次对称群 S_{48}(此群的阶为48!)的一个子群——魔方群.魔方是一个由27个小方块组合的正方体,每个面都可转动.如图,在小方块外露的面上标以数字.则顺时针转1,2,3,4所在的面时,便得到如下的置换

$$a = (1\ \ 2\ \ 3\ \ 4)(5\ \ 6\ \ 7\ \ 8)(12\ \ 32\ \ 40\ \ 20)$$
$$(21\ \ 13\ \ 26\ \ 34)(19\ \ 11\ \ 31\ \ 39)$$

而魔方群也就是由下面计算程序中的 a, b, c, d, e, f 六个置换在 S_{48} 中生成的子群.



下面是用MAPLE计算魔方群时,计算机屏幕上的显示记录.魔方群的2-Sylow子群是指它的阶为 2^{27}(2的最大可能幂)的子群.这里给出它的11-Sylow子群.

```
> with(group);
[DerivedS, LCS, NormalClosure, RandElement, Sylow, areconjugate, center, centralizer,
core, cosets, cosrep, derived, groupmember, grouporder, inter, invperm, isabelian,
isnormal, issubgroup, mulperms, normalizer, orbit, permrep, pres]
```

```
> pg: = permgroup(48,{
  a={[1,2,3,4],[5,6,7,8],[12,32,40,20],[21,13,26,34], [19,11,31,39]],
> b=[[9,10,11,12],[13,14,15,16],[24,44,27,7],[18,46,32,1], [45,29,2,19]],
> c=[[17,18,19,20],[21,22,23,24],[9,1,39,48],[14,6,33,43], [12,4,38,45]],
> d=[[29,30,31,32],[25,26,27,28],[46,37,3,11],[41,35,8,16], [47,40,2,10]],
> e=[[37,38,39,40],[33,34,35,36],[48,20,3,30],[42,22,5,25], [47,17,4,31]],
> f=[[45,46,47,48],[41,42,43,44],[17,9,29,37],[23,15,28,36], [18,10,30,
    38]]});
pg := permgroup(48,{
a =[[1,2,3,4],[5,6,7,8],[12,32,40,20], [21,13,26,34],[19,11,31,39]],
b =[[9,10,11,12],[13,14,15,16],[24,44,27,7], [18,46,32,1],[45,29,2,19]],
c =[[17,18,19,20],[21,22,23,24],[9,1,39,48], [14,6,33,43],[12,4,38,45]],
d =[[29,30,31,32],[25,26,27,28],[46,37,3,11], [41,35,8,16],[47,40,2,10]],
e = [[37,38,39,40],[33,34,35,36],[48,20,3,30], [42,22,5,25],[47,17,4,31]],
f = [[45,46,47,48],[41,42,43,44],[17,9,29,37], [23,15,28,36],[18,10,30,38]]})
> grouporder(pg);
                    43252003274489856000
> with(numtheory);
> ifactor(43252003274489856000);
                        27    14    3    2
                    (2)   (3)   (5)   (7)   (11)
> Sylow(pg,11);
  permgroup(48,{[[5,22,21,25,44,27,24,8,41,7,23],
            [6,35,15,16,14,26,28,13,43,34,33]]})
```

在本节最后,我们给出下面

定理 4.3 (A. Cayley,1821—1895) 设 G 是阶为 n 的群,则 G 同构于 n 元对称群 S_n 的一个子群.

证明 任取 $a\in G$,利用它如下地作一个集 G 到集 G 的映射 T_a:

$$T_a:\ G\longrightarrow G$$
$$x\longmapsto xa,$$

T_a 是集 G 到集 G 的一个单射,因为 $x\neq y$,当然也有 $xa\neq ya$. 有限集 G 到自身的一个单射永远是满射,故 T_a 是 n 个元素的集 G 到自身上的一个一一对应,即 $T_a\in S_n$. 令 $T=\{T_a,a\in G\}$,则由 $xT_{ab}=x(ab)=(xa)b=(xT_a)T_b=x(T_aT_b)$,得 $T_{ab}=T_aT_b$,由之还得 $T_aT_{a^{-1}}=T_{aa^{-1}}=T_e=T_{a^{-1}a}=T_{a^{-1}}T_a$,即 $T_a{}^{-1}=T_{a^{-1}}$,总起来便知集 T 关于乘法和取逆封闭,即 T 是 S_n 的一个子群. 令

$$\begin{aligned} \phi: \quad G &\longrightarrow T \\ a &\longmapsto T_a, \end{aligned}$$

当 $a \neq b, eT_a = ea = a, eT_b = eb = b$，即 $T_a \neq T_b$，故 ϕ 是单射. 再由 $T_{ab} = T_aT_b$，即 $\phi(ab) = \phi(a)\phi(b)$，故得 ϕ 是群 G 到群 T 的同构. □

注意到上面证明中，当 G 是无限群时，T_a 也是 G 到自身的一个变换，故也有

定理 4.4 设 G 是任意群，则 G 同构于变换群 $T(G)$ 的一个子群.

这个用 Cayley 命名的定理给出一个抽象群 G 和另一个具体群 S_n 的关系，即任一 n 阶群都和 n 元对称群 S_n 的一个子群同构，也就是说，如果我们能把 S_n 中所有不同构的 n 阶子群都找出来，这样我们也就把所有可能存在的 n 阶群都找出来了. 把研究抽象群归结为研究置换群(即对称群 S_n 的子群). 当然给人一些良好感觉，例如对寻找群的例子或讨论某些问题是会有帮助的，但它不会给我们很多，而只是研究群的一种途径，这也是我们可以感觉到的.

练习

1. 设 $G = \langle a \rangle$ 是有限循环群. 如果 a 的阶 n 为偶数，证明：存在元素 $e \neq b \in G$，使得 b 是 G 的所有自同构的不动点，即对任意 $f \in \mathrm{Aut}(G)$，有 $f(b) = b$.

2. 设 $B_4 = \{e, a, b, c\}$ 是四元群，其群 B_4 的乘法由下列乘法表给出

	e	a	b	c
e	e	a	b	e
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

此时称 B_4 为 Klein 四元群. 试将 B_4 用对称群 S_4 中的置换表示出来. 并把这些置换写成不相交的轮换的乘积形式.

§5 商群

关于集合，在集合论中我们有集合的等价关系，划分以及商集的概念. 关于群，它们的相应概念将是什么呢？

回忆一下集合论中等价关系，划分和商集的概念.

设 M 是一个集合,称 $M\times M$ 到 $\{1,0\}$ 的一个映射 ϕ 为集 M 的一个关系.任取 $x,y\in M$,当 $\phi(x,y)=1$ 时称 x,y 有关系 ϕ,记作 $x\phi y$,当 $\phi(x,y)=0$ 时,称 x,y 没有关系 ϕ.

定义 5.1 称集 M 的一个关系 ϕ 为一个等价关系,如果 ϕ 满足下列三条:

E1) 自反律:对任意 $x\in M$,有 $x\phi x$;

E2) 对称律:对任意 $x,y\in M$,若 $x\phi y$,则 $y\phi x$;

E3) 传递律:对任意 $x,y,z\in M$,若 $x\phi y, y\phi z$,则 $x\phi z$.

定义 5.2 称集 M 的一些子集的集合 $\Psi=\{M_i\mid i\in I\}$,其中 I 是(有限或无限)脚码集,为集 M 的一个划分,如果 Ψ 满足下列两条:

D1) $M_i, i\in I$,中任意两个互不相交;

D2) $M=\bigcup\limits_{i\in I}M_i$.

这时,如果把 M_i 作为一个整体,当作一个新元素看待,则把由这些元素 $M_i, i\in I$,组成的集合(仍记作)$\Psi=\{M_i\mid i\in I\}$ 称作集 M 的一个商集.

我们知道,集合 M 的一个等价关系确定 M 的一个划分,反之也对.现在的问题是如何把这些概念移植到群,一个带有运算的集合上去.这里的原则是简单的:一切要和运算和谐,要保持运算关系.

定义 5.3 设 G 是一个群.集 G 的一个等价关系 ϕ 称作群 G 的一个合同关系,如果对任意 $x,y,u,v\in G$,若 $x\phi y$ 及 $u\phi v$,则 $(x\cdot u)\phi(y\cdot v)$.

设 $\Psi=\{M_i\mid i\in I\}$ 是集 G 的一个划分.对于任意取定的 $a\in G$,划分 Ψ 中有且仅有一个子集 M_i 包含 a,我们把这个子集 M_i 记作 $[a]$,即 $[a]$ 是含 a 的那个子集.但应特别注意的是,当 a,b 都属于 M_i 时,则有 $M_i=[a]=[b]$,即这个表示法不是唯一的:对于 G 中不同元素 a,b,可能有 $[a]$ 和 $[b]$ 是表示同一个子集的.无论如何,我们可把划分 $\Psi=\{M_i\mid i\in I\}$ 改记为 $\Psi=\{[a]\mid a\in G\}$.当然这时我们应把重复出现的元素看成一个,例如集合 $\{1,1,1,2,3,2\}$ 就是集合 $\{1,2,3\}$,它只含 3 个元素而不是 6 个元素.

定义 5.4 设 G 是一个群.集 G 的一个划分 $\Psi=\{[a]\mid a\in G\}$ 称作 G 的一个合同划分,如果对任意 $a,b\in G$,有

$$[a]\cdot[b]\subseteq[ab]. \tag{1}$$

在这里我们重复一下群 G 中两个子集 H,K 的乘积 $H\cdot K$ 的定义:

$$H\cdot K=\{xy\mid x\in H, y\in K\}.$$

这样,(1)是说,若 $x\in[a], y\in[b]$,则必有 $xy\in[ab]$,也就是说,若 x_1,x_2 同属于 Ψ 中的一个子集,y_1,y_2 同属于 Ψ 中的一个子集,则 x_1y_1 和 x_2y_2 也必同属于 Ψ 中的一个子集.

有了这些定义后,可以设想群的合同关系与群的合同划分之间有和集的等价关系与集的划分完全类似的联系.是复习也是证明新结果,我们给出

命题 5.5 1) 设 ϕ 是群 G 的一个合同关系.对 $a \in G$,令

$$[a] = \{x \in G \mid x\phi a\},$$

则 $\Psi = \{[a] \mid a \in G\}$ 是群 G 的一个合同划分;

2) 设 $\Psi = \{[a] \mid a \in G\}$ 是群 G 的一个合同划分.在集 G 中如下地引入一个关系 ϕ:对 $x, y \in G$ 规定 $x\phi y$ 当且仅当存在 $a \in G$,使得 $x, y \in [a]$,则 ϕ 是群 G 的一个合同关系.

证明 1) 由于 ϕ 也是集 G 的一个等价关系,故 Ψ 是集 G 的一个划分.任取 Ψ 中两个元素 $[a], [b], a, b \in G$,今往证:$[a] \cdot [b] \subseteq [ab]$.首先由 $a\phi a$,有 $a \in [a]$.任取 $x \in [a], y \in [b]$,则由 $x\phi a, y\phi b$ 以及 ϕ 是合同关系,可知 $xy\phi ab$,即 $xy \in [ab]$,因而有

$$[a] \cdot [b] = \{xy \mid x \in [a], y \in [b]\} \subseteq [ab],$$

即命题中的 1)得证.

2) 由于 Ψ 也是集 G 的一个划分,故 2)中定义的 ϕ 是集 G 的一个等价关系.若有 $x\phi y, u\phi v$,这说明存在 $a, b \in G$,使得 $x, y \in [a]$ 而 $u, v \in [b]$.但由于 Ψ 是合同划分,故有 $[a][b] \subseteq [ab]$,因而 xu, yv 都在 $[ab]$ 中.依 ϕ 的定义,得 $(xy)\phi(uv)$,即命题中的 2)得证. □

这样,群的合同关系和合同划分就是一回事了,即是用两种语言——关系或子集——描写同一事物.

下面我们看一个简单例子.

例 1 在群 $(\mathbf{Z}, +)$ 中考虑下面关系:取定正整数 $n > 1$,规定:$\mathbf{Z}$ 中两数 s, t 有模 n 同余关系 $\sim$,当且仅当 $n \mid (s - t)$,这就是 $s \sim t$ 当且仅当 s, t 被 n 除时有同样的余数.容易证明,$\sim$ 是集 $\mathbf{Z}$ 的一个等价关系,且若 $s_1 \sim s_2, t_1 \sim t_2$,则也有 $(s_1 + t_1) \sim (s_2 + t_2)$.这样 $\sim$ 是群 $\mathbf{Z}$ 的一个合同关系.它所对应的合同划分

$$\Psi = \{[i] \mid i \in \mathbf{Z}\} = \{[s] \mid 0 \leqslant s \leqslant n-1\}$$

是由 G 中下列子集组成:

$$[s] = \{mn + s \mid m \in \mathbf{Z}\}, \quad s = 0, 1, 2, \cdots, n-1,$$

特别 $[0] = \{mn \mid m \in \mathbf{Z}\}$, $[1] = \{mn + 1 \mid m \in \mathbf{Z}\}$.

直接验证一下 Ψ 是个合同划分也是很有益的.例如直接看出这些 $[s]$ 彼此不相交,任何整数必属于某一 $[s]$,如 $-2 \in [n-2]$ 等等,因而 Ψ 是个划分.另外不难证明:对 $0 \leqslant s, t \leqslant n-1$,

$$[s]+[t]\subseteq\begin{cases}[s+t], & \text{当 } s+t\leqslant n-1,\\ [s+t-n], & \text{当 } s+t\geqslant n.\end{cases}\tag{2}$$

这些都是我们在初等整数论中学习同余关系时所熟悉的.

设 G 是一个群, ϕ 是群 G 的一个合同关系,而 $\Psi=\{[a]\mid a\in G\}$ 是与 ϕ 相应的合同划分.把这些 G 的子集 $[a]$ 看成元素,今在由元素 $[a],a\in G$ 组成的集合 Ψ 中,利用群 G 的运算 ·,引入 Ψ 的一个运算 $\times$ 如下:规定 Ψ 中两个元素 $[a]$ 和 $[b]$ 的乘积为 Ψ 中的元素 $[ab]$, 即规定

$$[a]\times[b]=[ab].\tag{3}$$

在这个规定中我们利用 $[a]$ 中的一个特定代表 a 和 $[b]$ 中的一个特定代表 b. 如果选用 $[a]$ 中另一个元素 x 和 $[b]$ 中另一个元素 y, 即有 $[a]=[x]$, $[b]=[y]$, 依规定我们将得到

$$[x]\times[y]=[xy].$$

因而我们必须证明 $[ab]=[xy]$, 否则上面规定就不给出 Ψ 的一个运算,因为相同的元素 $[a]=[x],[b]=[y]$ 依该规定得不同的结果.

若用合同划分语言去证,由定义 5.4(1)得, $x\in[a],y\in[b]$, 则 $xy\in[a]\cdot[b]\subseteq[ab]$, 即 $xy\in[ab]$, 因而 $[xy]=[ab]$.

若用合同关系语言去证,这就是,若 $x\in[a],y\in[b]$, 则 $x\phi a,y\phi b$, 因而依定义 5.3 得 $xy\phi ab$, 因而 xy 和 ab 同属一个子集,即 $\times$ 是集 Ψ 的一个运算.

定理 5.6 $(\Psi,\times)$ 是一个群.

证明 已证 $\times$ 是 Ψ 的一个运算,由

$$([a]\times[b])\times[c]=[ab]\times[c]=[(ab)c],$$
$$[a]\times([b]\times[c])=[a]\times[bc]=[a(bc)],$$

以及在群 G 中有 $(ab)c=a(bc)$, 便得 $\times$ 适合结合律.

$[e]$, e 是群 G 的恒等元,起恒等元的作用: $[e]\times[a]=[ea]=[a]$, $[a]\times[e]=[ae]=[a]$.

再由 $[a]\times[a^{-1}]=[aa^{-1}]=[e]=[a^{-1}]\times[a]$ (即 $([a])^{-1}=[a^{-1}]$) 知 G4)也满足. □

定义 5.7 我们称上定理中的群 $(\Psi,\times)$ 为群 G 的(由合同划分 Ψ, 或由合同关系 ϕ 确定的)一个商群.

当不会引起混淆时,我们常把 Ψ 的运算 $\times$ 也写成 ·.

例 1(续一) $\Psi=\{[i]\mid i\in\mathbf{Z}\}$, 此时上面(3)规定的 Ψ 的运算,仍记为 +, 就是

$$[i]+[j]=[i+j].$$

依定理 5.6 知 $(\Psi, +)$ 是一个群，群 Ψ 的阶是 n. 把这个整数加群 $\mathbb{Z}$ 的商群记作 $\mathbb{Z}_n$. $\mathbb{Z}_n$ 是 n 阶循环群，$[1]$ 是它的生成元.

容易证明：$\mathbb{Z}_n$ 和 §3 的例 6 中的 $C_n = \langle \rho_\theta \rangle, \theta = \frac{2\pi}{n}$ 是同构的.

我们会找出一个群的所有商群吗？也就是问，我们会找出一个群的所有合同关系吗？

集合是一盘散沙，集合的等价关系是千形百状，没有什么规律的. 然而，群的合同关系，是与运算和谐(或保持运算)的那些等价关系，是非常有规律的.

设 $\Psi = \{[a], a \in G\}$ 是群 G 的一个合同划分，其相应的合同关系为 ϕ. 恒等元 e 是群 G 的一个非常特殊的元素，先看 $[e]$，我们有 $[e] \cdot [e] \subseteq [e]$，故 G 的子集 $[e]$ 关于 G 的运算封闭. 任取 $a \in [e]$，则由 $a\phi e, a^{-1}\phi a^{-1}$ 得 $aa^{-1}\phi ea^{-1}$，即 $e\phi a^{-1}$，即 $a^{-1} \in [e]$. 这样 $[e]$ 是 G 的一个子群. 再由对任意 $a \in G$，有

$$a[e]a^{-1} \subseteq [a][e][a^{-1}] \subseteq [aea^{-1}] = [e],$$

故知 $[e]$ 是 G 的一个正规子群.

再看 $[a]$，我们有：$a[e] \subseteq [a][e] \subseteq [a]$. 另一方面还有 $a^{-1}[a] \subseteq [a^{-1}][a] \subseteq [e]$，再用 a 左乘其两侧，则有

$$aa^{-1}[a] \subseteq a[e], \qquad 即 \quad [a] \subseteq a[e].$$

这样合起来便得 $[a] = a[e]$，即是 $\Psi = \{a[e] \mid a \in G\}$ 而 $[e]$ 是正规子群.

反过来，我们从群 G 的一个子群 H 出发，而考虑 G 中所有形如 $aH, a \in G$ 的子集全体 Ψ，即 $\Psi = \{aH \mid a \in G\}$. 今证 Ψ 是集合 G 的一个划分. 由于 $a = ae \in aH$，故 $G = \bigcup_{a \in G} aH$. 其次，若 $aH \cap bH$ 不空，即有 $x \in aH \cap bH$，因而有 $h_1, h_2 \in H$，使得 $x = ah_1, x = bh_2$，即 $ah_1 = bh_2$. 故有 $ah_1h_2^{-1} = bh_2h_2^{-1}$，即 $b = ah_1h_2^{-1}$. 由于 H 是子群，$HHH \subseteq H$，故我们有下面包含关系：

$$bH = ah_1h_2^{-1}H \subseteq aHHH \subseteq aH.$$

对称地可得 $aH \subseteq bH$，即有 $aH = bH$. 这就证明了：在这些子集 $aH, a \in G$ 中或者两个完全相同，或者两个之交是空集. 总起来，便得 $\Psi = \{aH \mid a \in G\}$ 是集 G 的一个划分. 类似地可得 $\{Ha \mid a \in G\}$ 也是集 G 的一个划分.

形如 aH(H 是子群)的子集是群 G 中重要的一类子集.

定义 5.8　设 H 是群 G 的子群，称 $aH(Ha)$ 为子群 H 的左(右)陪集. 而称 $\{aH \mid a \in G\}$ 为子群 H 的左陪集系.

当 H 只是子群而不是正规子群时，$\Psi = \{aH \mid a \in G\}$ 只是集 G 的划分，

不会是群 G 的合同划分，因为若 Ψ 是，则 Ψ 中的 $[e]$（此时 $[e]=H$）该是正规子群. 即 H 为正规子群是 Ψ 为合同划分的必要条件.

今取 H 为正规子群，而往证：$\Psi=\{aH \mid a\in G\}$ 是群 G 的合同划分. 由上面已知 Ψ 是集 G 的划分，只需证这个划分是保持运算的. 注意到 $\forall\ a\in G, aH=Ha$. 故有

$$aH\cdot bH=a(Hb)H=ab(HH)\subseteq abH.$$

证明完成.

注意到对子群 H 言，有 $H\cdot H=H$（为什么?）故上式可改进为

$$aH\cdot bH=abH.$$

综合上述讨论：在群 G 的正规子群的全体和群 G 的合同划分（合同关系）的全体之间有一个一一对应，这就是 $H\longmapsto\{aH \mid a\in G\}$，亦即 G 的正规子群的（左）陪集系给出 G 的所有可能的合同划分，因而也就给出 G 的所有商群. 把正规子群 H 的陪集系 $\{aH \mid a\in G\}$ 确定的商群记作 G/H，亦即 $G/H=(\{aH \mid a\in G\},\times)$，其运算规则是：$aH\times bH=abH$.

例 1（续二） 整数加群 $\mathbf{Z}$ 是一个交换群，因而它的每一个子群都是正规子群. 不难找出 $\mathbf{Z}$ 的所有子群. 任取它的一个子群 $H\neq\langle 0\rangle$，令 n 是 H 中正整数的最小者，则 H 中任一正整数 m 必都是 n 的倍数，否则余数 $r=m-qn\in H$（因为 $m,n\in H$）且 $0<r<n$ 而得矛盾. 这样 $H=\langle n\rangle$，即群 $\mathbf{Z}$ 的子群都是循环群.

$H=\langle n\rangle$ 的陪集系 $\{sH=[s] \mid s\in\mathbf{Z}\}$，这里 $[s]=\{mn+s \mid m\in\mathbf{Z}\}$，所作成的商群 $\mathbf{Z}/\langle n\rangle$ 就是本例在前面讨论过的群 $\mathbf{Z}_n=\Psi=\{[i] \mid i\in\mathbf{Z}\}$. 这样 $\mathbf{Z}_n, n\in\mathbf{Z}^+$，给出加群 $\mathbf{Z}$ 的所有真商群（指不等于 $\mathbf{Z}$ 者）.

这样，关于循环群分类的定理 3.3 可改述为：整数加群 $\mathbf{Z}$ 及其商群 $\mathbf{Z}_n, n\in\mathbf{Z}^+$ 给出所有可能的循环群.

正规子群 H 和商群 G/H 是群论中最重要的基本概念. 让我们再总结一下：

商群 G/H 就是：$G/H=\{aH, a\in G\}$. 而运算为：$aH\times bH=abH$.

练习

1. 设 G 是群，$\psi=\{[a] \mid a\in G\}$ 是群 G 的一个合同划分. 证明：对任意 $a,b\in G$，有子集的相等 $[a]\cdot[b]=[ab]$.

2. 设 H 是群 G 的非空子集. 在 G 中定义关系 $x\sim y$ 当且仅当 $xy^{-1}\in H$. 证明：

 1）$\sim$ 是等价关系当且仅当 H 是 G 的子群；

 2）$\sim$ 是合同关系当且仅当 H 是 G 的正规子群.

3. 固定一个正实数 a. 对任意实数 $x\in\mathbf{R}$. 记 $[x]=\{na+x \mid n\in\mathbf{Z}\}$ 和 $\psi=$

$\{[x] \mid x \in \mathbb{R}\}$.

1) 证明 ψ 是加群 $(\mathbb{R}, +)$ 的一个合同划分.

2) 记 $e^{i\theta} = \cos\theta + i\sin\theta$, 其中 θ 为实数, i 为虚数单位, 即 $i^2 = -1$. 那么 $C = \{e^{i\theta} \mid \theta \in \mathbb{R}\}$ 在通常复数乘法"·"之下形成一个群(称为单位元群). 又记 $(\Psi, +)$ 是 1)中的商群. 证明:

$$\phi: \ (\Psi, +) \longrightarrow (C, \cdot)$$
$$[1] \longmapsto e^{i\frac{2n\pi}{a}}$$

是群同构.

§6 同态

现在来研究两个群之间的关系. 对于两个集合来说,它们之间的关系,当然就是指它们之间有些什么样的映射. 然而对于群 G 和群 H 言,我们只对集 G 和集 H 之间那些保持运算的映射感兴趣.

定义 6.1 给定 $(G, \cdot)$ 和群 $(H, \times)$. 称集 G 到集 H 的一个映射 $\phi: G \longrightarrow H$ 是群 G 到群 H 的一个同态映射(简称同态), 如果对任意 $g_1, g_2 \in G$ 有

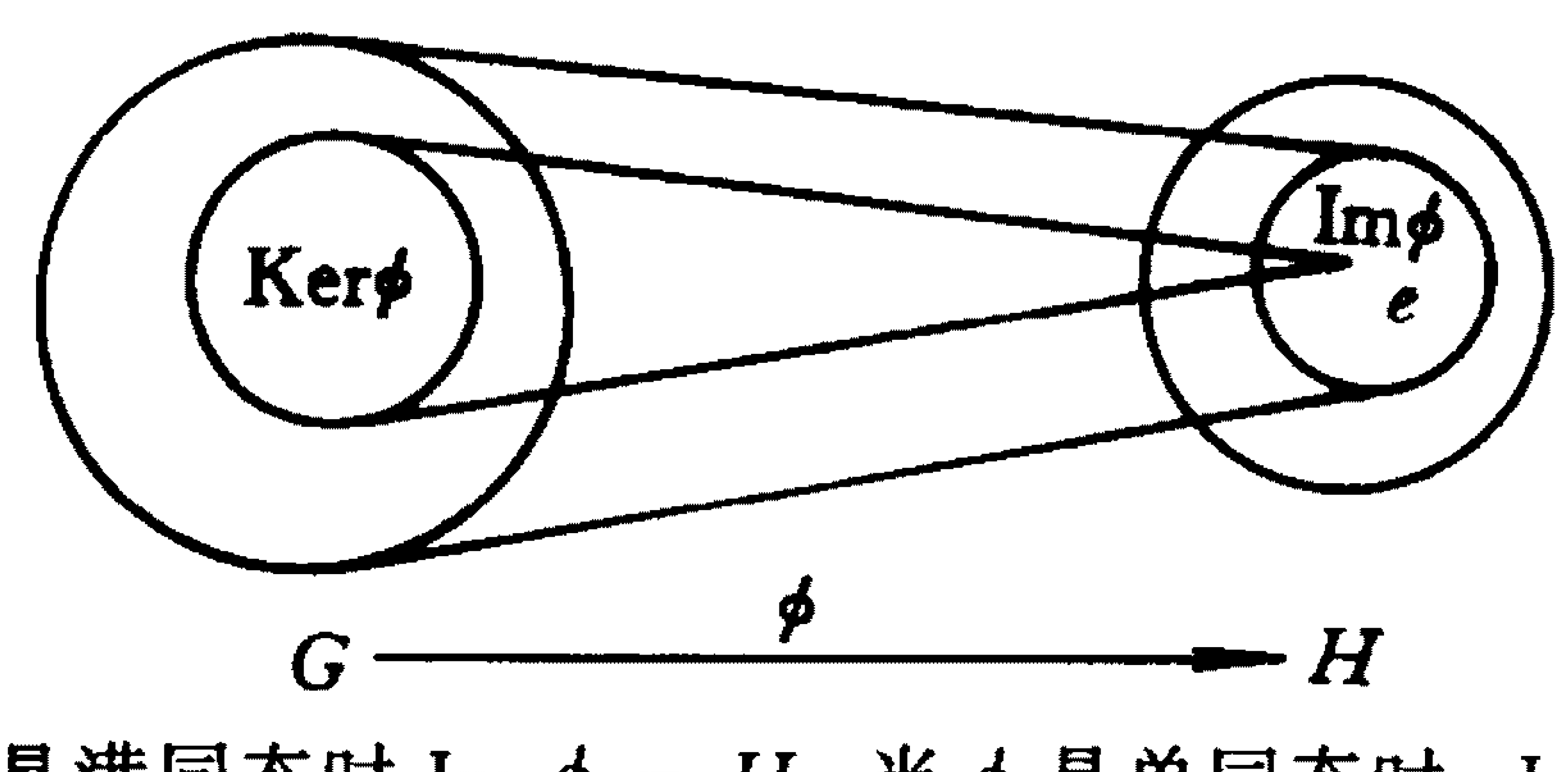
$$\phi(g_1 \cdot g_2) = \phi(g_1) \times \phi(g_2).$$

当 ϕ 是单(满)射时,称 ϕ 单(满)同态.

当 ϕ 是群 G 到群 H 的一个同态时, 令 $\{\mathrm{Im}\}\phi = \{\phi(g), g \in G\}$, 称之为 ϕ 的象, 或群 G 的同态象. 显然 $\{\mathrm{Im}\}\phi \subseteq H$. 令

$$\mathrm{Ker}\phi = \{x \in G \mid \phi(x) = e, e \text{ 是 } H \text{ 的恒等元}\},$$

称之为 ϕ 的核. 显然 $\mathrm{Ker}\phi \subseteq G$. 用图表示,就是



易见, 当 ϕ 是满同态时 $\mathrm{Im}\,\phi = H$, 当 ϕ 是单同态时, $\mathrm{Im}\phi = \{e\}$.

显然同态是同构的推广, 其差别是没有要求映射 ϕ 一定是一个到上的一一对应. 一个同态是同构当且仅当它既是单同态又是满同态.

例 1 (1)令

$$\phi: \ GL_n(\mathbb{R}) \longrightarrow (\text{非 0 实数全体,数的乘法})$$
$$A \longmapsto |A| \quad (\text{矩阵 } A \text{ 的行列式}).$$

易证，ϕ 是一个满射，并保持运算（$|A \cdot B| = |A| \cdot |B|$），故 ϕ 是一个满同态．此例中，$\mathrm{Ker}\phi = \{A \in GL_n(\mathbb{R}) \mid |A| = 1\}$，即 $\mathrm{Ker}\phi$ 是特殊线性群．

（2）令

$$\phi:(\text{非 0 实数全体，数的乘法}) \longrightarrow GL_n(\mathbb{R})$$
$$r \longmapsto rI_n(I_n \text{ 是 } n \text{ 阶单位矩阵}).$$

易证，ϕ 是一个单射并保持运算，故 ϕ 是一个单同态．此例中 $\mathrm{Im}\phi$ 由 $GL_n(\mathbb{R})$ 中所有纯量矩阵组成．

（3）令 H 是群 G 的一个子群，

$$\begin{aligned}\phi:\ H &\longrightarrow G\\ h &\longmapsto h.\end{aligned}$$

显然 ϕ 是群 H 到群 G 的一个单同态．

（4）令 H 是群 G 的正规子群，

$$\begin{aligned}\phi:\ G &\longrightarrow G/H = \{aH \mid a \in G\}\\ a &\longmapsto aH.\end{aligned}$$

ϕ 是一个满射，另一方面 $\phi(a) \times \phi(b) = aH \times bH = abH$，$\phi(ab) = abH$，即 ϕ 保持运算：$\phi(ab) = \phi(a) \times \phi(b)$，故 ϕ 是 G 到其商群 G/H 的一个满同态．常称之为 G 到 G/H 的自然满同态．

在本例中，$\mathrm{Ker}\phi = H$．

（5）令 $G = \langle a \rangle$ 是无限循环群，令

$$\begin{aligned}\phi:\ \langle a \rangle &\longrightarrow \mathbb{Z}_{12}\\ a^m &\longmapsto [3m], \qquad m \in \mathbb{Z}.\end{aligned}$$

ϕ 是一个映射，既不是单射，例如 $a^m \longmapsto [3m]$，$a^{m+12} \longmapsto [3m+36]$ 但 $a^m \neq a^{m+12}$，而在群 $\mathbb{Z}_{12}$ 中 $[3m] = [3m+36]$，也不是满射，例如 $\langle a \rangle$ 中没有元素对应 $\mathbb{Z}_{12}$ 中的 $[1]$．　ϕ 是保持运算的，因为

$$\begin{aligned}\phi(a^m) + \phi(a^p) &= [3m] + [3p] = [3(m+p)]\\ &= \phi(a^{m+p}) = \phi(a^m \cdot a^p).\end{aligned}$$

故 ϕ 是一个同态，但既不是单同态，也不是满同态．在本例中 $\mathrm{Im}\phi = \{[3m] \mid m \in \mathbb{Z}\} = \{[3],[6],[9],[0]\}$ 有 4 个元素，而 $\mathrm{Ker}\phi = \langle a^4 \rangle$．

和同构一样，关于同态也有

命题 6.2　ϕ 是群 G 到群 H 的一个同态，则有

$$\phi(e) = e, \quad \phi(a^{-1}) = \phi(a)^{-1}.$$

证明　先证 $\phi(e) = e$（当然左侧的 e 是 G 的恒等元，右侧的 e 是 H 的恒等元）．由 $e\phi(e) = \phi(e) = \phi(e \cdot e) = \phi(e) \cdot \phi(e)$，消去 $\phi(e)$ 便得 $e =$

$\phi(e)$. 其次,由

$$e=\phi(e)=\phi(aa^{-1})=\phi(a)\phi(a^{-1}),$$
$$e=\phi(e)=\phi(a^{-1}a)=\phi(a^{-1})\phi(a),$$

即得 $\phi(a^{-1})=\phi(a)^{-1}$. □

命题 6.3 ϕ 是群 G 到群 H 的同态,则有:

1) $\mathrm{Im}\phi$ 是群 H 的子群;

2) $\mathrm{Ker}\phi$ 是群 G 的正规子群.

证明 1) 任取 $h_1,h_2\in\mathrm{Im}\phi=\{\phi(g),g\in G\}$, 则依集 $\mathrm{Im}\phi$ 的定义,必有 $g_1,g_2\in G$, 使得 $h_1=\phi(g_1),h_2=\phi(g_2)$. 这时 $h_1h_2=\phi(g_1)\phi(g_2)=\phi(g_1g_2)\in\mathrm{Im}\phi$, $h_1^{-1}=\phi(g_1)^{-1}=\phi(g_1^{-1})\in\mathrm{Im}\phi$, 即集 $\mathrm{Im}\phi$ 是 H 的子群.

2) 任取 $g_1,g_2\in\mathrm{Ker}\phi=\{g\in G\,|\,\phi(g)=e\}$, 则 $\phi(g_1g_2)=\phi(g_1)\phi(g_2)=e\cdot e=e,\phi(g_1^{-1})=\phi(g_1)^{-1}=e^{-1}=e$, $\phi(ag_1a^{-1})=\phi(a)\phi(g_1)\phi(a^{-1})=\phi(a)\cdot e\cdot\phi(a)^{-1}=e$, 即得 $\mathrm{Ker}\phi$ 是群 G 的正规子群.
□

定理 6.4(群的第一同态定理) 1) 若群 H 是群 G 的正规子群,则

$$\begin{aligned}\phi:\ G&\longrightarrow G/H\\ g&\longmapsto gH\end{aligned}$$

是群 G 到其商群 G/H 的满同态.

2) 设 ϕ 是群 G 到群 $\overline{G}=\mathrm{Im}\phi$ 的满同态,而 $H=\mathrm{Ker}\phi$, 则 $G/H\cong\overline{G}$.

证明 关于 1),见例 1(4). 现证 2). 令 $H=\ker\phi$, H 是 G 的正规子群,商群 $G/H=\{gH,g\in G\}$. 令

$$\begin{aligned}\theta:\ G/H&\longrightarrow \overline{G}\\ gH&\longmapsto \phi(g).\end{aligned}$$

首先验证 θ 是集 G/H 到 $\overline{G}$ 的一个映射:若 $gH=g'H,g,g'\in G$, 必有 $\phi(g)=\phi(g')$, 即 gH 的象与 gH 的代表元素 g 的选择无关. 由于 $g'\in gH$, 故存在 $h\in H,g'=gh$, 这样

$$\phi(g')=\phi(gh)=\phi(g)\phi(h)=\phi(g)\cdot e=\phi(g).$$

再证 θ 是单的,即要证:若 $\phi(g_1)=\phi(g_2)$, 则 $g_1H=g_2H$. 由于

$$\begin{aligned}\phi(g_1^{-1}g_2)&=\phi(g_1^{-1})\phi(g_2)\\&=\phi(g_1)^{-1}\phi(g_2)=\phi(g_1)^{-1}\phi(g_1)=e,\end{aligned}$$

故 $g_1^{-1}g_2\in\mathrm{Ker}\phi=H$, 而有 $g_2\in g_1H$, 即 $g_2H=g_1H$. 最后由于 ϕ 是满射, $\mathrm{Im}\phi=\{\phi(g)\,|\,g\in G\}=\overline{G}$, 而由 θ 之定义知 $\mathrm{Im}\theta$ 也等于 $\{\phi(g),g\in G\}$, 故 θ 是满射. 至此证得 θ 是 G/H 到 $\overline{G}$ 上的一一对应.

至于 θ 保持运算,则是很容易得到的:

$$\theta(g_1H\cdot g_2H)=\theta(g_1g_2H)=\phi(g_1g_2)=\phi(g_1)\phi(g_2)$$
$$=\theta(g_1H)\cdot\theta(g_2H).\quad\square$$

群 G 的同态象 $\overline{G}$ 可以设想为群 G 的一个“粗略”的模型：忽略了 G 中某些元素间的差异而又维持 G 中的运算关系. 上述定理说，群 G 的所有可能的“粗略”模型就是群 G 的那些商群.

保持运算的同态映射当然把群 G 中所有运算关系（指涉及元素和运算的所有等式）都传递给 G 的同态象 $\overline{G}$，所以 $\overline{G}$ 保持着 G 中的某些结构. 例如，若 G 是交换群，则 $\overline{G}$ 也是；若在 G 中所有元素的阶都小于 n，则在 $\overline{G}$ 中所有元素的阶也都小于 n. 反过来当然不对，有时 $\overline{G}$ 交换，而 G 是非交换群（见上例中(1)），$\overline{G}$ 中元素的阶都小于或等于 n，而 G 中除 e 外每一元素的阶都是 ∞（见上例中(5)）. 下面定理说明了群与它商群的子群之间的关系.

定理 6.5（群的第二同态定理） 设 ϕ 是群 G 到群 $\overline{G}$ 上的满同态，$H=\mathrm{Ker}\phi$. 令

$L(G,H)=\{G$ 中所有包含 H 的子群$\}$，

$L(\overline{G})=\{\overline{G}$ 中所有子群$\}$，

则

$$\theta:\ L(G,H)\longrightarrow L(\overline{G})$$
$$S\longmapsto \phi(S)=\{\phi(s),s\in S\}=\overline{S}$$

是集 $L(G,H)$ 到集 $L(\overline{G})$ 上的一个一一对应，且有

(1) $S\supseteq T$ 当且仅当 $\phi(S)\supseteq\phi(T)$.

(2) S 是 G 的正规子群当且仅当 $\phi(S)$ 是 $\overline{G}$ 的正规子群.

(3) 当 S 是 G 的正规子群时，有

$$G/S\cong\overline{G}/\phi(S).$$

我们把这个有趣定理的证明留给读者.

证明这个定理所需要的方法和技巧都在前面出现过，能给出它的证明说明你已经很好地掌握子群、正规子群、商群和同态这些群论中最重要、最基本的概念. 多复习，多查一查前面的东西，你一定能证出来的.

如果说两国之间有政治关系、经济关系等等许多关系，则对于两个群之间的关系就只有同态关系. 单同态意味着甲群与乙群的一个子群一样（同构），满同态说明乙群就是甲群的商群，非单非满的同态，则是说甲群的一个商群和乙群的一个子群是一样的. 这样同态关系是群的仅有关系，而子群、商群是这种

关系仅涉及的两个基本语言.

练习

1. 设 ϕ 是群 G 到群 H 的一个同态. 设 M 和 N 分别是 G 和 H 的非空子集, 记 $\phi(M) = \{\phi(a) \mid a \in M\}$, 称为 M (在 ϕ 之下) 的象, 记 $\phi^{-1}(N) = \{a \in G \mid \phi(a) \in N\}$, 称为 N (在 ϕ 之下) 的完全原象. 证明:

1) 如果 S 是 G 的子群, 那么 S 的象 $\phi(S)$ 是 H 的子群.

2) 如果 T 是 H 的子群, 那么 T 的完全原象 $\phi^{-1}(T)$ 是 G 的子群. 进一步, 如果 T 是 H 的正规子群, 那么 $\phi^{-1}(T)$ 是 G 的正规子群.

3) 如果 S 是 G 的子群, 那么 $\phi^{-1}(\phi(S)) = S \cdot \mathrm{Ker}\phi$.

2. 证明定理 6.5.

3. 设 $\phi: G \to H$ 是群 G 到群 H 的一个群同态, S 是 G 的子群. 定义

$$\begin{aligned} \phi': \quad S &\longrightarrow \phi(S) \\ s &\longmapsto \phi(s). \end{aligned}$$

证明:

1) ϕ' 是群的满同态(称为由 ϕ 限制在 S 上导出的群满同态);

2) $\mathrm{Ker}\phi' = S \cap \mathrm{Ker}\phi$;

3) 有群同构 $S \cap \mathrm{Ker}\phi \cong \phi(S)$. 特别地, 如果 $S \supseteq \mathrm{Ker}\phi$, 那么有群同构 $S/\mathrm{Ker}\phi \cong \phi(S)$.

4. 设 G 是群, H 是 G 的正规子群, S 是 G 的子群. 证明

1) SH 是 G 的子群. 并且 H 是 SH 的正规子群. 也有 $S \cap H$ 是 S 的正规子群;

2) 有群同构 $SH/H \cong S/S \cap H$.

§7 有限群

有限群尽管是只有有限个元素的群, 然而其内容是非常丰富、非常深刻的. 有限群不同于无限群当然就在于其阶是一个正整数 n. 围绕着这个数 n, 对一般有限群的元素、子群、正规子群、商群等可得许多数量性质, 可提出许多问题. 进一步的讨论, 该从有限群类划分出一些子类, 而对这些子类中的群研究其结构; 另一方面应该研究一个给定有限群和其他具体群, 特别是矩阵群之间的关系, 即所谓有限群的表示问题.

在本节中 G 表示有限群, 其阶 $|G| = n$.

首先研究 G 的阶 n 和其元素的阶, 其子群的阶, 其商群的阶之间的数量关系.

命题 7.1 (J. L. Lagrange, 1736 - 1813) 设 G 的子群 H 的阶为 m, 则

$m \mid n = |G|$.

证明　我们有 $G = \bigcup_{g \in G} gH$，设 H 的不同左陪集的个数为 t，则 G 是 t 个两两不相交的形如 gH 的子集的并集. 另一方面 H 的左陪集 gH 所含元素个数和 H 的一样多，因为 H 中不同元素，左乘以同一元素 g 后当然还是不同的（应用消去律），即 $|gH| = |H| = m$. 合起来便得 $n = |G| = t \cdot m$. □

注意到阶为 m 的元素 a 所生成的子群 $\langle a \rangle$ 的阶也为 m，便得

推论 7.2　1）有限群 G 的元素 a 的周期 m 必整除 $|G| = n$；

2）对有限群 G 的任意元素 a 都有 $a^n = e$.

定义 7.3　设 H 是 G 的子群，H 的不同左陪集的个数为 t. 我们称 t 是子群 H 在 G 中的指数，简称为子群 H 的指数.

这样，我们有公式：

有限群 G 的阶 = 子群 H 的阶 × 子群 H 的指数.

由之看到不但子群的阶是群的阶的因数，子群的指数也是.

推论 7.4　若 H 是 G 的正规子群，则有 $|G| = |H| \cdot |G/H|$.

很自然会问：任给 n 的因数 m，在 G 中存在元素 a，其阶为 m 吗？或者退一步，在 G 中存在子群 H，其阶为 m 吗？

讨论存在性问题，总是较困难的，一般讲，上面问题的回答是否定的，然而在某些条件下，例如有限交换群，我们能得到肯定结果.

先从最简单的循环群入手.

引理 7.5　在阶为 n 的循环群 $\langle a \rangle$　$(a^n = e)$ 中，对任意正整数 $m \mid n$，都有子群 H，H 的阶是 m.

证明　设 $n = mt$，考察 $\langle b \rangle$，其中 $b = a^t$. 易见 $b^m = (a^t)^m = a^{tm} = a^n = e$. 而对任意正整数 $s < m$，有 $ts < n$，故 $b^s = (a^t)^s = a^{ts} \neq e$，即得 b 的阶为 m，随之 $\langle b \rangle$ 之阶为 m. □

引理 7.6　设 G 是有限交换群，其阶 $n = pm$ 其中 p 为素数. 则在 G 中存在阶为 p 的元素.

证明　对 m 作归纳. 当 $m = 1$ 时，结论显然成立. 设 $m > 1$，任取 $e \neq a \in G$，记 $H = \langle a \rangle$. 若 $p \mid |H|$，由 H 为有限循环群和引理 7.5 知 H 中存在，从而 G 中存在阶为 p 的元素. 若 $p \nmid |H|$，记 $\overline{G} = G/H$ 为 G 的商群. 则 $|\overline{G}| = |G|/|H| = pm'$，其中 $1 \leqslant m' < m$. 由归纳假设知存在 $b \in G$ 使得 bH 在 $\overline{G}$ 中的阶为 p. 于是 $b \notin H$ 但 $b^p \in H$. 设 a 的阶为 s，则 $p \nmid |H| = s$ 且 $(b^s)^p = (b^p)^s = e$. 另一方面 $b^s \neq e$，这是因为若 $b^s = e$，则由 p, s 互素，故有整数 q, r 使 $qp + rs = 1$，这时 $b = b^{qp} \cdot b^{rs} = (b^p)^q \in H$，与前面 $b \notin H$

相矛盾. 故 b^s 的阶为 p. □

命题 7.7　设 G 是有限交换群,其阶 $|G| = n$. 则对任意 $m|n$, 存在 G 的子群 H 使得 $|H| = m$.

证明　对 m 作归纳,不妨设 $m > 1$. 设 p 为素数且 $p|m$. 由引理 7.6 知 G 中存在阶为 p 的元素,记为 a. 考虑商群 $\overline{G} = G/\langle a\rangle$. 由 $\frac{m}{p} \mid \frac{n}{p}$ 和归纳假设知 $\overline{G}$ 中存在子群 $\overline{H}$ 使得 $|\overline{H}| = \frac{m}{p}$. 记 H 为 $\overline{H}$ 在 G 到 $\overline{G}$ 的自然满同态之下的完全原象. 那么 H 是 G 的子群, 且 G 到 $\overline{G}$ 的自然满同态在 H 上的限制导出 H 到 $\overline{H}$ 的满射, 是群的满同态且核也为 $\langle a\rangle$. 故 $|H| = |\langle a\rangle| \cdot |\overline{H}| = p \cdot \frac{m}{p} = m$, 即 H 为所求的子群. □

这样对有限交换群,我们肯定地回答了上面提出的问题.

对一般有限群的子群存在问题,我们只讨论下面的问题:若素数的幂 $p^r|n$, 在阶为 n 的群 G 中是否存在子群 H, 其阶为 p^r. 为此,除了用元素的阶、群的阶和指数去计算外,我们还需要引入一些新概念,它们都是很基本很有用的.

定义 7.8　设 G 为任意群(即不一定是有限群),

(1) 说 G 中元素 a, b 是共轭的,若存在 $g \in G$ 使 $b = gag^{-1}$, 亦即存在 $\phi \in \mathrm{Inn}G$, 使 $b = \phi(a)$. 易见共轭关系是一个等价关系,称它的一个等价类, 亦即 $\{gag^{-1}, g \in G\}$, 为一个共轭元素类.

(2) 说 G 的子群 H, K 共轭,若存在 $g \in G$ 使 $K = gHg^{-1}$, 亦即存在 $\phi \in \mathrm{Inn}G$, 使 $K = \phi(H)$. 共轭关系是子群间的一个等价关系,称它的一个等价类,亦即 $\{gHg^{-1}, g \in G\}$, 为一个共轭子群类.

定义 7.9　设 S 是群 G 的一个子集,令

$$N(S) = \{g \in G \mid gSg^{-1} = S\},$$

称为集 S 的正规化子.

易见 $N(S)$ 是 G 的一个子群.

从上面定义立即知道,一个中心元自己组成一个共轭元素类,而一个中心元 c 的正规化子 $N(c) = G$. 若 S 是群的子群,则 $S \subseteq N(S)$, 且 S 是群 $N(S)$ 的正规子群, $N(S)$ 还是 G 中子群有此性质者中的最大的.(证明!)若 S_i, $i \in I$ 是 G 的所有不同的共轭元素类,由于共轭是等价关系,故这些 S_i 两两不相交,且它们的并集等于 G, 即 $G = \bigcup_i S_i$.

引理 7.10　G 是有限群, S 是 G 的一个共轭元素类, $|S| = t$. 则存在 G 的子群 H, 它在 G 中的指数恰为 t.

证明　任取 $s \in S$ 而考察 s 的正规化子 $N(s)$. 由子群 $N(s)$ 的定义易知

$$xsx^{-1} = ysy^{-1} \Longleftrightarrow s = (x^{-1}y)s(y^{-1}x) = (x^{-1}y)s(x^{-1}y)^{-1}$$
$$\Longleftrightarrow x^{-1}y \in N(s) \Longleftrightarrow x,y \text{ 属于 } N(s) \text{ 的同一左陪集}$$

亦即用 $N(s)$ 的同一左陪集中的元素去作用 s 给出 s 的相同共轭元素，而用不同左陪集中的元素去作用 s，则给出 s 的不相同的共轭元素. 这样 s 的不同共轭元素的个数就等于子群 $N(s)$ 的不同左陪集的个数，亦即 $|S|$ 等于子群 $N(s)$ 在群 G 中的指数. □

定理 7.11(Sylow 定理) 设 G 是有限群，其阶 $n = p^r \cdot m$，其中 p 为素数，那么存在 G 的子群 H 使得 $|H| = p^r$.

证明 对 n 作归纳. 设 C 是 G 的中心. 由命题 7.7 可设 $C \neq G$. 若 $p \mid |C|$，由引理 7.6 知 C 中存在 p 阶子群 $\langle a\rangle$. 当然 $\langle a\rangle$ 是 G 的正规子群. 考虑商群 $\overline{G} = G/\langle a\rangle$. 由归纳假设知 $\overline{G}$ 中存在 p^{r-1} 阶子群 $\overline{H}$. 记 H 是 G 到 $\overline{G}$ 的自然满同态之下的完全原象. 那么 H 是 G 的子群，且 $|H| = |\langle a\rangle| \cdot |\overline{H}| = p \cdot p^{r-1} = p^r$，即 H 为所求的子群. 设 $p \nmid |C|$. 设 $C_i, i = 1,2,\cdots,t$，是 G 的所有不同的共轭元素类. 注意元素的共轭关系是一个等价关系，故 G 等于所有 C_i 的不交并. 从而

$$n = |G| = \sum_{i=1}^{t} |C_i| = n_1 + \cdots + n_t, \tag{1}$$

其中 $n_i = |C_i|, i = 1,2,\cdots,t$. 易见 $n_i = 1$ 当且仅当 C_i 由一个元素 g_i 组成，而后者当且仅当 g_i 是中心元. 于是(1)又可写成

$$n = |G| = |C| + m_1 + \cdots + m_s, \tag{2}$$

其中 $s \geqslant 1$ 且对每个 $1 \leqslant j \leqslant s$ 存在某个共轭元素类 C_i 使得 $m_j = |C_i| > 1$. 由 $p \nmid |C|$ 知存在某个 m_j 使得 $p \nmid m_j$. 取共轭元素类 C_i 使得 $m_j = |C_i|$. 由引理 7.10 知存在 G 的子群 N 使得 $|C_i| = [G:N]$. 故由 $p \nmid m_j$ 和 $p^r m = |G| = |N| \cdot [G:N] = |N| \cdot m_j$ 知 $p^r \mid |N|$. 然而 $m_j > 1$ 蕴含着 $|N| < |G|$. 故由归纳假设知存在 N 的子群 H 使得 $|H| = p^r$. 当然 H 也是 G 的 p^r 阶子群. □

证明中的(2)式称为有限群 G 的类方程.

推论 7.12 G 是有限 p - 群，即 G 是有限群且每个元素的阶是素数 p 的某次幂，当且仅当 G 的阶为 p 的幂. □

上面的定理即是著名的 Sylow 第一定理. 它肯定了有限群 G 的阶为素数 p 的幂的所有子群中存在极大者，称为 G 的 Sylow p - 子群. 关于 Sylow p - 子群的个数以及它们之间的关系，有很完整的结果. 我们下面叙述这个群论中非常漂亮的结果而略去证明，供读者欣赏.

定理(Sylow) G 是有限群，其阶 $n = p^s \cdot m$，其中 p, m 互素，p 是素数，则

1) 群 G 中存在有 t 个 Sylow p - 子群,即阶为 p^s 的子群,其中 $t\mid m$, $t\equiv 1 \pmod{p}$;

2) 群 G 中所有 Sylow p - 子群彼此共轭,即所有 Sylow p - 子群组成一个共轭子群类.

练习

1. 设 G 是 p 阶群,其中 p 为素数.证明:对任意 $a\in G$,若 $a\neq e$,则 $G=\langle a\rangle$.

2. 设 G 是群,证明: G 的指数为 2 的子群 H 为正规子群.

3. 设 p 为素数.

1) 设 $\mathbf{Z}_p=\{[i]\mid i=0,1,2,\cdots,p-1\}$ 是模 p 的剩余类加群.在 $\mathbf{Z}_p\setminus\{[0]\}$ 中定义乘法 $[i][j]=[ij]$.证明: $\mathbf{Z}_p\setminus\{[0]\}$ 在此乘法之下构成一个 $p-1$ 阶群;

2) (Fermat) 证明:对任意整数 a,有 $a^p\equiv a \pmod{p}$.

4. 设 S 是有限群 G 的子集.记 $O(S)=\{gSg^{-1}\mid g\in G\}$,即 $O(S)$ 是 G 中所有与 S 共轭的子集的集合.证明: $|O(S)|=[G:N(S)]$.其中 $|O(S)|$ 表示集合 $O(S)$ 中元素的个数.

§8 有限交换群的结构定理

本节中我们将看到非常漂亮完整的有限交换群的结构定理.由之我们将具体地理解到,什么是群的结构理论.

在本节中 G 表示交换群,群的运算记作加法"+",简称 G 为加群.

在加群 G 中我们已经知道 ng $(g\in G, n\in\mathbf{Z})$ 的意义.我们可以把它解释成 $\mathbf{Z}\times G$ 到 G 的一个运算 ·,即规定 $n\cdot g=ng$.这个运算 · 显然满足下列性质:对任意 $g,h\in G,n,m\in\mathbf{Z}$,有

M1) $n\cdot(g+h)=n\cdot g+n\cdot h$;

M2) $(n+m)\cdot g=n\cdot g+m\cdot g$;

M3) $(nm)\cdot g=n\cdot(m\cdot g)$;

M4) $1\cdot g=g$.

这样,我们眼中的加群 G 就变成一个和数域 F 上向量空间 V 相类似的对象了,只不过在向量空间 V 中谈论线性和时其系数取自数域 F,而对加群 G 言,我们也可以谈论线性和

$$m_1\cdot g_1+\cdots+m_s\cdot g_s,$$

但系数只能取自整数环 $\mathbf{Z}$.

把加群 G 和向量空间 V 的类比是很有好处的.例如向量空间 V 的基本

概念、两个向量集等价的概念等都能很容易地移植到加群 G 上来.

设子集 $H=\{h_1,\cdots,h_t\}\subseteq G$，而规定

$$\mathbb{Z}\cdot H=\{n_1\cdot h_1+\cdots+n_t\cdot h_t\mid,n_i\in\mathbb{Z},1\leqslant i\leqslant t\},$$

易见 $\mathbb{Z}\cdot H=\langle H\rangle$，即 $\mathbb{Z}\cdot H$ 就是 H 生成的子群. 并且当 $H=\{g_1,\cdots,g_t\}$ 是群 G 的生成元集时，

$$G=\mathbb{Z}\cdot H=\mathbb{Z}\cdot g_1+\cdots+\mathbb{Z}\cdot g_t.$$

下面的概念在结构理论中起着重要作用.

定义 8.1(内直和的定义) 设 G 是加群，而 H_i，$1\leqslant i\leqslant t$ 是 G 的子群. 若

1) $G=H_1+\cdots+H_t$，即每一 g 都可表成 $h_1+\cdots+h_t$，$h_i\in H_i$.

2) 若对任意 $g\in G$，由 $g=h_1+\cdots+h_t=h'_1+\cdots+h'_t,h_i,h'_i\in H$，必有 $h_i=h'_i$，$i=1,\cdots,t$，亦即这种表示法是唯一的.

则称 G 是子群 $H_1,\cdots,H_t$ 的(内)直和，记作 $G=H_1\oplus H_2\oplus\cdots\oplus H_t$. 此时也称 G 可分解为子群 $H_1,\cdots,H_t$ 的直和.

显然，群的直和与向量空间的直和是很类似的概念.

将下面常用到的一些事实，写成

引理 8.2 在加群 G 中，

1) 若元素 g 的阶为 t，而 $(t,s)=1$，则 sg 的阶亦为 t 且 $\langle g\rangle=\langle sg\rangle$.

2) 若元素 g 的阶为 t，而 $(t,s)=k$，则 sg 的阶为 t/k.

3) 若 $g_1+\cdots+g_m=0$ 且 g_i 的阶 t_i，$i=1,2,\cdots,m$，两两互素，则每个 $g_i=0$.

证明 只证 3). 对 m 作归纳. 不妨设 $m>1$. 则 $t_mg_1+\cdots+t_mg_{m-1}=0$. 对任意 $1\leqslant i\leqslant m-1$，由 $(t_m,t_i)=1$ 和 1)知 t_mg_i 的阶也是 t_i. 故由归纳假设知 $t_mg_i=0$. 又由 $(t_m,t_i)=1$ 知 $g_i=0$. 即 $g_1=g_2=\cdots=g_{m-1}=0$. 从而也有 $g_m=0$. □

命题 8.3 设 G 是有限加群，$|G|=n=p_1^{m_1}p_2^{m_2}\cdots p_t^{m_t}$，其中 p_i 是不同素数. 则有

1) $G=H_1\oplus\cdots\oplus H_t$，其中 H_i 是 p_i－群，$i=1,\cdots,t$；

2) 若 $G=G_1\oplus\cdots\oplus G_t=G'_1\oplus\cdots\oplus G'_t$，其中 G_i,G'_i 是 p_i－群，$i=1,\cdots,t$，则对任意 i，有 $G_i=G'_i$.

证明 1) 对任意 $1\leqslant i\leqslant t$，令 $n_i=p_i^{m_i},r_i=\dfrac{n}{n_i},H_i=\{g\in G\mid g$ 的阶是 p_i 的幂$\}$. 那么易知 $H_i=\{g\in G\mid n_ig=0\}$. 易证 H_i 是 G 的子群. 从而易知 $H_1+H_2+\cdots+H_t=\{h_1+h_2+\cdots+h_t\mid h_i\in H_i,i=1,2,\cdots,t\}$ 是 G

的子群. 任取 $a \in G$, 注意到 $r_1, r_2, \cdots, r_t$ 的最大公因子是 1, 由初等数论知, 存在整数 $s_1, s_2, \cdots, s_t$ 使得 $\sum_{i=1}^{t} s_i r_i = 1$, 令 $b_i = s_i r_i a$, 则 $a = (\sum_{i=1}^{t} s_i r_i) a = \sum_{i=1}^{t} b_i$. 由 G 的阶为 n 知 $na = 0$. 故 $n_i b_i = s_i r_i n_i a = s_i na = 0$, 即 $b_i \in H_i$, $i = 1, 2, \cdots, t$. 故 $a \in H_1 + H_2 + \cdots + H_t$. 于是 $G = H_1 + \cdots + H_t$. 由定义知 H_i 是 p_i - 群. 这就证明了 1).

易知定义 8.1 中的 2) 等价于: 若 $h_1 + \cdots + h_t = 0$, 这里 $h_i \in H_i$, 则必有 $h_i = 0$, $i = 1, 2, \cdots, t$. 而由引理 8.2 3) 知这是成立的, 因为 h_i 的阶为 p_i 的幂, 而它们是两两互素的. 故 $G = H_1 \oplus H_2 \oplus \cdots \oplus H_t$. □

上命题把有限加群的研究归结为对有限 p - 加群的研究.

设 G 为加群且 $|G| = n = p^m$, p 是素数. 我们想更精细地分解它.

如果 $G = \langle g \rangle = \mathbb{Z}g$ 是循环群, 则 G 不能再分解, 因为若

$$G = \mathbb{Z}g = \mathbb{Z}g_1 \oplus \mathbb{Z}g_2, \quad |\mathbb{Z}g_1| = p^{m_1}, |\mathbb{Z}g_2| = p^{m_2}, m_1 \leqslant m_2 < m,$$

则 $p^{m_2}G = 0$, 这和 g 的阶是 p^m 相矛盾. 这样从直和的角度来看, 循环 p - 群是最基本的构件了, 它相当于向量空间中的一维空间.

因而最好的结果将是把 p - 加群 G 表成循环群的直和.

假设我们有

$$G = \mathbb{Z}g_1 \oplus \cdots \oplus \mathbb{Z}g_k,$$

我们想知道 $\{g_1, \cdots, g_k\}$ 这个 G 的生成元集在 G 的所有生成元集中有一些什么特殊的地位和性质, 从而能使我们利用它把这个特殊的生成元集找出来. 和向量空间的基相比较, 容易想到这将是元数最小的生成元集. 另一点将想到的是 g_i 的阶 p^{m_i} 组成的集合 $\{p^{m_1}, \cdots, p^{m_k}\}$ 该有点什么"极端"的性质.

设 $\{g_1, \cdots, g_k\}$, $\{h_1, \cdots, h_k\}$ 是 G 的两个元素个数相等的生成元集, 其相应的阶集依次为 $\{p^{m_1}, \cdots, p^{m_k}\}$, $\{p^{l_1}, \cdots, p^{l_k}\}$, 如果

$$m_1 + \cdots + m_k < l_1 + \cdots + l_k,$$

我们就说生成元集 $\{g_1, \cdots, g_k\}$ 小于生成元集 $\{h_1, \cdots, h_k\}$.

命题 8.4 G 为有限 p - 加群, $|G| = p^m$. 则有

1) $G = \mathbb{Z}g_1 \oplus \cdots \oplus \mathbb{Z}g_k$,

2) 若 $G = \mathbb{Z}g_1 \oplus \cdots \oplus \mathbb{Z}g_k = \mathbb{Z}h_1 \oplus \cdots \oplus \mathbb{Z}h_s$, 则必 $k = s$ 且适当重排脚码后有 $\mathbb{Z}g_i \cong \mathbb{Z}h_i$, $i = 1, \cdots, k$.

证明 1) 显然 G 有有限生成元集, 因而有元素个数最小(说是 k)的生

成元集，在这些元素个数最小的生成元集中，必有一按上面规定的大小关系是极小的生成元集，任取其中一个，记作 $\{g_1,\cdots,g_k\}$，其相应阶集为 $\{p^{r_1},\cdots,p^{r_k}\}$. 对生成元集言，显然有：$G=\mathbb{Z}g_1+\cdots+\mathbb{Z}g_k$.

今证 $G=\mathbb{Z}g_1\oplus\cdots\oplus\mathbb{Z}g_k$.

用反证法，若不然，则有(不妨设为三项) $i<j<t$，

$$l_ig_i+l_jg_j+l_tg_t=0,\ l_ig_i,l_jg_j,l_tg_t \text{ 都不等于 } 0, \tag{1}$$

若 l_i 不被 p 整除，此时 l_i 和 g_i 的阶互素，则有

$$l_ig_i=-l_jg_j-l_tg_t,$$

$$\mathbb{Z}g_i=\mathbb{Z}(l_ig_i)\subseteq\mathbb{Z}g_j+\mathbb{Z}g_t,$$

上式中第一个等号的根据是引理 8.2. 这时从元数最小的生成元集 $\{g_1,\cdots,g_k\}$ 中去掉元素 g_i 后仍是生成元集，这是不可能的. 故不妨设 l_i,l_j,l_t 都被 p 整除. 设 $(l_i,l_j,l_t)=p^sl$，其中 p 与 l 互素，$s\geqslant1$，则(1)可改写成

$$p^s(m_ig_i+m_jg_j+m_tg_t)=0,$$

m_i,m_j,m_t 中必有一个不被 p 整除，不妨设为 m_j，这时由引理8.2，m_jg_j 和 g_j 的阶相等，都是 p^{r_j}. 考察元素集

$$M=\{g_1,\cdots,g_{j-1},g'_j=m_ig_i+m_jg_j+m_tg_t,g_{j+1},\cdots,g_k\}.$$

重复上面讨论，可知 M 是 G 的生成元集，其元素个数为 k，仍是最小元素个数者. 另一方面，$p^sm_jg_j=l_jg_j\neq0$ 因而 $p^s<p^{r_j}$，但 $p^sg'_j=0$，g'_j 的阶 $\leqslant p^s$，这样按上面规定的次序，应有 $\{g_1,\cdots,g_k\}$ 大于 M，但这和我们对 $\{g_1,\cdots,g_k\}$ 的选择是矛盾的. 证完 1).

2) 设 $\mathbb{Z}g_1\oplus\cdots\oplus\mathbb{Z}g_k=\mathbb{Z}h_1\oplus\cdots\oplus\mathbb{Z}h_s$. 对 g_i 的个数 k 作归纳法. $k=1$ 时，由于 p －循环群不能再分解，故 $s=1$ 且 $\mathbb{Z}g_1\cong\mathbb{Z}h_1\cong G$. 设 $k>1$，且不妨设所有 g_i 中 g_k 的阶最大，记 g_k 的阶为 p^m. 易知所有 h_i 的阶中的最大数也是 p^m，否则用前面证明 p －循环群不可分解的方法可得出矛盾. 下面写出元素 g_k 用元素 h_i 表示的表达式：

$$g_k=l_1h_1+\cdots+l_sh_s, \tag{2}$$

不妨设 $h_j,h_{j+1},\cdots,h_s$ 是 h_i 中所有阶为 p^m 的元素，则它们在(2)中的系数 l_t，$t=j,j+1,\cdots,s$，不能都被 p 整除，否则 g_k 的阶将小于 p^m. 不妨设 $(l_s,p)=1$，这时使用上面用过的方法，读者可以证明

$$G=\mathbb{Z}h_1\oplus\mathbb{Z}h_2\oplus\cdots\oplus\mathbb{Z}h_{s-1}\oplus\mathbb{Z}g_k.$$

另一方面，我们有

$$G=\mathbb{Z}g_1\oplus\mathbb{Z}g_2\oplus\cdots\oplus\mathbb{Z}g_{k-1}\oplus\mathbb{Z}g_k.$$

考察商群 $\overline{G}=G/\mathbb{Z}g_k\cong\mathbb{Z}g_1\oplus\cdots\oplus\mathbb{Z}g_{k-1}\cong\mathbb{Z}h_1\oplus\cdots\oplus\mathbb{Z}h_{s-1}$. 利用归纳

法假设,便得 $k-1=s-1$,并且适当调整脚码后,有 $\mathbb{Z}g_i \cong \mathbb{Z}h_i, i=1,2,\cdots,k-1$. 另一方面,$g_k$ 和 $h_s=h_k$ 同为阶为 p^m 的元素,当然也有 $\mathbb{Z}g_k \cong \mathbb{Z}h_k$. 定理全部证完.□

上述两个命题说明,任意给定的有限加群必是阶为素数幂的循环群的直和.应该看一下问题的另一面,即存在性问题:是否存在有限加群,它是,例如说,4 个 8 阶循环群和 7 个 125 阶循环群的直和? 为了回答这个问题,我们引入

定义 8.5 (外直积的定义) 设 $G_i, i=1,\cdots,n$,是(任意)群,令集合 $G=G_1\times G_2\times\cdots\times G_n$,而规定集 G 中的一个二元运算如下:对 $g_i,h_i\in G_i, i=1,2,\cdots,n$,规定

$$(g_1,g_2,\cdots,g_n)\cdot(h_1,h_2,\cdots,h_n)=(g_1h_1,g_2h_2,\cdots,g_nh_n),$$

这里 g_ih_i 当然是按群 G_i 中的运算得到的乘积.直接验证 $(G,\cdot)$ 是一个群,称之为群 G_i, $i=1,\cdots,n$ 的(外)直积,记作 $G=G_1\otimes G_2\otimes G_3\otimes\cdots\otimes G_n$. 特别,当所有 G_i 是交换群时,易见 $G=G_1\otimes G_2\otimes\cdots\otimes G_n$ 也是交换群.我们常把 G 写成 $G=G_1\oplus\cdots\oplus G_n$ 而称之为加群 G_i 的(外)直和.这时 G 的运算记作加法,而写成

$$\begin{aligned}&(g_1,g_2,\cdots,g_n)+(h_1,h_2,\cdots,h_n)\\&=(g_1+h_1,g_2+h_2,\cdots,g_n+h_n),\end{aligned}$$

当然 g_i+h_i 是指按 G_i 的加法得到的和.令

$$G'_i=\{(0,\cdots,0,g_i,0,\cdots,0)\mid g_i\in G_i\},$$

易见 G'_i 是 G 的子群,$G'_i\cong G_i$,且按定义 8.1 有 G 是其子群 G'_i, $i=1,2,\cdots,n$,的(内)直和.在这个意义上内直和,外直和是互通的,虽然内直和概念是属于结构理论的,而外直和是属于构造理论的.

上面的讨论肯定地回答了刚才所提出的关于有限加群的存在问题.

总结以上我们有下面这个漂亮的结果.

定理 8.6(有限交换群结构定理) 有限加群 G 可唯一地分解为素数幂循环群的直和,即设 $|G|=p_1^{m_1}p_2^{m_2}\cdots p_t^{m_t}$, p_i 是不同素数,则

1) $G=G_{11}\oplus\cdots\oplus G_{1s_1}\oplus\cdots\oplus G_{t1}\oplus\cdots\oplus G_{ts_t}$,其中 G_{ij} 是阶为 $p_i^{m_{ij}}$ 的循环群;

2) 自然数集 $(p_1^{m_{11}},\cdots,p_1^{m_{1s_1}},\cdots,p_t^{m_{t1}},\cdots,p_t^{m_{ts_t}})$ 由群 G 唯一确定.

这是一个很值得玩味的结构定理.你可以把它和算术基本定理相比.那里表示任意整数的基本构件是"素数",构造方法是"乘积",而这里则是:表示任意有限加群的基本构件是"素数幂阶的循环群",构造方法是"直和".在整数论中,自然数 n 的分解是 $n=p_1^{m_1}p_2^{m_2}\cdots p_t^{m_t}$,则在交换群论中,有限加群 G

的阶 $|G| = n$ 的分解将是:

$$|G| = n = p_1^{m_{11}} \cdots p_1^{m_{1s_1}} \cdots p_t^{m_{t1}} \cdots p_t^{m_{ts_t}}.$$

如果把 n 的因数和 G 的子群相类比,虽然我们不能用此结构定理找出 G 的所有子群,然而利用它却可容易地再一次证明下面

命题 8.7　G 是有限加群, $|G| = n$ 而 $m \mid n$. 则 G 中必有阶为 m 的子群. □

下面留给读者的是一个大习题,用这里的方法去证明线性代数中我们熟悉的矩阵的 Jordan 标准形的存在性. 这是很有意思的事:有限加群的结构定理和矩阵的 Jordan 标准形的存在性是相通的,这里的关键是模论的语言.

以下用 R 表示整数环 $\mathbb{Z}$ 或数域 F 上一元多项式环 $F[x]$ (如果你能有抽象环的概念,可把 R 理解为有单位元 1 的环),说成: R 是环.

定义 8.8　R 是环, M 是加群,还有一个 $R \times M$ 到 M 的运算 $\cdot$, 如果此运算 $\cdot$ 满足下列条件:对任意 $a, b \in R, u, v \in M$ 有

M1) $a \cdot (u + v) = a \cdot u + a \cdot v$;

M2) $(a + b) \cdot u = a \cdot u + b \cdot u$;

M3) $(ab) \cdot u = a \cdot (b \cdot u)$;

M4) $1 \cdot u = u$.

则称 M 为环 R 上的模,记作 R - 模.

例 1　有限交换群 G, 依本节开头的解释,可看成是 $\mathbb{Z}$ - 模.

例 2　设 T 是复数域 $\mathbb{C}$ 上 n 维向量空间 V 的一个给定线性变换. 利用这个 T, 我们规定 $\mathbb{C}[x] \times V$ 到 V 的一个运算 $\cdot$:对任意 $f(x) \in \mathbb{C}[x], v \in V$,

$$f(x) \cdot v = f(T)v,$$

即规定 $f(x) \cdot v$ 为 v 在线性变换 $f(T)$ 下的象. 直接验证知,在此运算下加群 V 成为 $\mathbb{C}[x]$ - 模.

和加群的子群、商群,直和、同态等概念类似,我们可以定义 R - 模 M 的子模、商模、直和、同态等概念. 先引入一个符号: N 是 R - 模 M 的子集,规定

$$R \cdot N = \{a_1 u_1 + \cdots + a_n u_n \mid \forall\ a_i \in R, u_i \in N, \forall\ n \in \mathbb{N}\},$$

即 $R \cdot N$ 是以 R 中元素作系数, N 中元素的一切线性和的全体.

R - 模 M 的子集 N 称作 M 的 R - 子模,如果 $R \cdot N \subseteq N$ (此时 N 当然也是加群 M 的子群).

若 N 是 R - 模 M 的 R - 子模,考虑商加群 $M/N = \{u + N, u \in M\}$, 规定 $R \times M/N$ 到 M/N 的运算 $\cdot$: $a \cdot (u + N) = a \cdot u + N, a \in R, u \in M$. 直接验证可知,这个规定与陪集 $u + N$ 的代表元素 u 的选择无关,即若

$$u + M = v + M,$$

则必有(证明!)

$$a \cdot u + M = a \cdot v + M,$$

也就是 · 的确是一个运算.直接验证知,关于此运算 ·,加群 M/N 成为 R -模,称之为 R -模 M 关于 R -模 N 的商模.

读者不难给出关于 R -模的内直和和外直和的定义.

$\mathbb{Z}$-模 M 的元素 u 的阶规定为非零整数集 $\{n \mid n \cdot u = 0\}$ 中最小正数.容易证明元素 u 的阶是自然数,是唯一的.

$\mathbb{C}[x]$ -模 V 的元素 v 的阶规定为首项系数为 1 的多项式集 $\{f(x) \mid f(x) \cdot v = 0\}$ 中的次数最小者.容易证明元素 v 的阶是首 1 多项式,是唯一的.

把有限交换加群结构定理的证明,用 $\mathbb{Z}$-模语言写出便可证得下面的

定理 A 设 $\mathbb{Z}$-模 M 满足下面两个条件:

a) $M = \mathbb{Z} \cdot N, N \subseteq M$, N 是一个有限集(就是说,$\mathbb{Z}$-模 M 有一个有限生成元集,或 M 是有限生成的);

b) 存在正整数 n 使得对任意 $u \in M$,有 $n \cdot u = 0$(就是说,$\mathbb{Z}$-模 M 是一个周期 $\mathbb{Z}$-模).

则 $\mathbb{Z}$-模 M 可唯一分解成 $\mathbb{Z}u_i, i = 1,2,\cdots,s$,的直和,其中元素 u_i 的阶是素数幂.

因为上面定理中关于 $\mathbb{Z}$-模 M 的讨论用到的关于 $\mathbb{Z}$ 的算术性质,如唯一分解定理,对互素整数 m,n,必有整数 s,t 使得 $sn + tm = 1$ 等等,在 $\mathbb{C}[x]$ 中都相应的成立,因此把这个讨论平行地对 $\mathbb{C}[x]$ -模 V 进行,便得到下面定理的证明.

定理 B 设 $\mathbb{C}[x]$ -模 V 满足下面两个条件:

a) $V = \mathbb{C}[c] \cdot U, U \subseteq V, U$ 是一个有限集;

b) 存在非零多项式 $f(x)$ 使得对任意 $v \in V$,有 $f(x) \cdot v = 0$.

则 $\mathbb{C}[x]$ -模 V 可唯一地分解成 $\mathbb{C}[x] \cdot v_i, i = 1,2,\cdots,s$,的直和,其中元素 v_i 的阶是不可约多项式(一次多项式)的幂.

结合线性代数中的知识,把定理 B 应用于上面的例 2,便得到关于矩阵的 Jordan 标准形的存在性.

练习

1. 设 G 是群(未必交换),$H_1, H_2, \cdots, H_n$ 是 G 的子群.如果满足:

a) $G = H_1 H_2 \cdots H_n$;

b) 对任意 $h_i, h'_i \in H_i$, $i = 1,2,\cdots,n$, 有 $(h_1,\cdots,h_n)(h'_1,\cdots,h'_n) =$

$(h_1h'_1)\cdots(h_nh'_n)$;

c) 若 $g = g_1g_2\cdots g_n = g'_1g'_2\cdots g'_n$，其中 $g_i, g'_i \in H_i$, $i = 1,2,\cdots,n$. 则 $g_i = g'_i$, $i = 1,2,\cdots,n$.（此时称 g_i 是 g 在 H_i 中的分量.）

那么称 G 是子群 $H_1,H_2,\cdots,H_n$ 的内直积. 证明：如果 G 是子群 $H_1,H_2,\cdots,H_n$ 的内直积，那么

1) 对任意 $h_i \in H_i$ 和 $h_j \in H_j$. 若 $i \neq j$，则 $h_ih_j = h_jh_i$.

2) H_i 是 G 的正规子群.

3) 若 $i_1,i_2,\cdots,i_n$ 是 $1,2,\cdots,n$ 的一个排列，则 G 也是 $H_{i_1},H_{i_2},\cdots,H_{i_n}$ 的内直积.

4) 定义 ϕ_i:
$$\begin{aligned}\phi_i:\quad G &\longrightarrow H_i\\ g &\longmapsto g_i\ (g_i \text{ 是 } g \text{ 在 } H_i \text{ 上的分量}),\end{aligned}$$

并称 ϕ_i 是 G 在 H_i 上的投影. 则投影 ϕ_i 是群的满同态且 $\mathrm{Ker}\phi_i = H_1\cdots H_{i-1}H_{i+1}\cdots H_n$.

2. 设群 G 是子群 $H_1,H_2,\cdots,H_n$ 的内直积. 记 $\overline{G} = H_1\otimes H_2\otimes\cdots\otimes H_n$ 是群 $H_1,\cdots,H_n$ 的外直积. 令

$$\begin{aligned}\phi:\quad \overline{G} &\longrightarrow G\\ (h_1,\cdots,h_n) &\longmapsto h_1\cdots h_n,\end{aligned}$$

证明：ϕ 是群同构对应.

3. 设 G 是群，H_1,H'_1,H_2 是 G 的子群. 如果 G 是 H_1 和 H_2 的内直积，也是 H'_1 和 H_2 的内直积. 证明：有群同构 $H_1 \cong H'_1$. 试举反例说明，通常 $H_1 = H'_1$ 不成立.

4. 设群 G 是循环子群 $\langle a_1\rangle,\cdots,\langle a_n\rangle$ 的内直积. 如果每个 a_i 的周期 $m_i \neq \infty$ 且 $m_1, m_2,\cdots,m_n$ 两两互素. 证明 G 是循环群.

§9 单群

在这一节中我们继续研究有限群 G. 研究一种从结构角度来看最简单，最基本的群类.

定义 9.1 一个群叫做单群，如果它不是恒等元群且没有非平凡的正规子群.

在前面我们已经知道，一个群 G 的同态象必是 G 的商群 G/H，H 是 G 的正规子群. 对于单群 G 来说，其正规子群只能是 $\{e\}$ 和 G，这样单群 G 的同态象就只能是由一个恒等元组成的群 $\{e\}$ 以及 G 本身. 同态象（可以想象为 G 的粗略模型）如此简单，说明群 G 的结构也会是相应地简单的. 因而单群可看作一个“最简单”的群类.

另一方面，任取一个有限群 G，设其阶为 $n > 1$. 令

$$\mathbb{N}_G = \{G \text{ 中所有阶小于 } n \text{ 的正规子群}\},$$

显然它不空，因为正规子群 $\{e\}$ 是它的一个成员. 这样在 $\mathbb{N}_G$ 中必有一个阶最

大的正规子群(可能不只有一个).取其一,记作 H, $|H| = m$. 由对 H 的选择,我们知道在 $\mathbb{N}_G$ 中不会有真包含 H 者,即不存在 G 的正规子群 X 满足

$$H \subsetneq X \subsetneq G. \tag{1}$$

今考察商群 G/H. 由(1)以及定理 6.5 知 G/H 是单群. 现在假定(a):我们知道所有的有限单群. 由于 $|H| = m < n$, 至少从数学归纳法的角度(即假定阶小于 $|G|$ 的群为已知,而来研究群 G)来看,又可以认定群 H 是已知的. 再假定(b):如果 H 是已知群而 G/H 是单群,我们有办法把群 G 完全确定下来,即知道 G 的一个正规子群 H, 又知道其商群 G/H 是单群,我们便能知道 G 本身. 这样,只要假定(a),(b)成立,那么一切有限群就在我们的掌握中了.

上面的分析,说明有限单群在有限群类中起"基本构件"的作用,而(b)在有限群论中起"基本构造方法"的作用. 虽然(b)至今仍是假定,并没能很好的解决它,但有限单群的"基本构件"的重要意义是可以肯定的.

命题 9.2 一个(有限或无限)群 G 没有非平凡子群当且仅当 G 是恒等元群或同构于 $\mathbb{Z}_p$, p 是一个素数.

证明 如果 $G \neq \{e\}$, 则有元素 $a \in G, a \neq e$. 子群 $\langle a \rangle \neq \{e\}$, 因而由假设 $G = \langle a \rangle$. 再由前面关于循环群的结果便得命题. □

命题 9.3 一个交换群 G 是单群当且仅当 $G \cong \mathbb{Z}_p$, p 是素数. □

寻求所有的非交换有限单群,经过几代人的努力,在 20 世纪 80 年代终于完成了:有两系列单群,这就是 n 元交代群 A_n, $n \geqslant 5$ 和所谓 Lie 型单群——一些由矩阵组成的群. 在这两系列之外还有 26 个有限单群——常称为散在单群. 例如其中之一称作魔鬼群的阶为 $2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 59 \cdot 71$, 约为 10^{54}. 有限单群的完全分类是 20 世纪数学中巨大成果之一,充分展现了有限群论的美妙以及人类智慧的高超.

下面我们证明 A_5 的单性以及 Lie 型单群中的一个例子.

首先看一下在 n 元对称群 S_n 中,一个 t - 轮换 $(i_1 \quad i_2 \quad \cdots \quad i_t)$ 在置换 Σ 作用下所得的元素,亦即 $\Sigma^{-1}(i_1 \cdots i_t)\Sigma$ 具有什么样子. 设

$$\Sigma = \begin{pmatrix} \cdots & i_1 & i_2 & \cdots & i_t & \cdots \\ \cdots & j_1 & j_2 & \cdots & j_t & \cdots \end{pmatrix},$$

则直接计算可知

$$\Sigma^{-1}(i_1 \cdots i_t)\Sigma = \begin{pmatrix} \cdots & j_1 & j_2 & \cdots & j_t & \cdots \\ \cdots & i_1 & i_2 & \cdots & i_t & \cdots \end{pmatrix}(i_1 \quad i_2 \quad \cdots \quad i_t)$$

$$\cdot\begin{pmatrix}\cdots & i_1 & i_2 & \cdots & i_t & \cdots\\ \cdots & j_1 & j_2 & \cdots & j_t & \cdots\end{pmatrix}$$
$$=(j_1\quad j_2\quad \cdots\quad j_t). \tag{1}$$

(1)给出一个很简单很有用的计算规则.(1)说明在 S_n 中所有 t - 轮换组成一个共轭元素类,即在 S_n 中 t - 轮换彼此共轭,而与 t - 轮换共轭的元素也必是 t - 轮换.这使我们对"共轭"的概念在具体群 S_n 中有一个具体的,形象的感受.

但如果在 A_5 中看一个元素 a 的共轭元素时,则要小心一点,因为这时我们只能用 A_5 中的置换,即偶置换 Σ 去作用a, 这是在讨论 A_5 中共轭关系时要注意的.

定理 9.4 5 元交代群 A_5 是一个有限单群.

证明 设 $H \neq \{e\}$ 是 A_5 的一个正规子群,而去证明 $H = A_5$. 在前面我们已知所有 3 - 轮换是 A_5 的一个生成元集.这样我们分两步去证:先证(a) H 中必至少有一个 3 - 轮换,再证(b) 所有 3 - 轮换也是 A_5 的一个共轭元素类,因而 H 含所有的 3 - 轮换.

易见 A_5 中除恒等元外只有三种形状:5 - 轮换,3 - 轮换以及两个对换的乘积.任取 $e \neq a \in H$, 若 a 是一个 5 - 轮换,不妨设 $a = (1\quad 2\quad 3\quad 4\quad 5)$. 取

$$\Sigma = \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 1 & 2 & 5 & 3 & 4\end{pmatrix} = (3\quad 5\quad 4) \in A_5,$$

计算得

$$H \ni \Sigma^{-1}a\Sigma$$
$$= (1\quad 2\quad 5\quad 3\quad 4),$$

再计算

$$\begin{aligned}H \ni \Sigma^{-1}a\Sigma \cdot a^{-1} &= (1\quad 2\quad 5\quad 3\quad 4)(1\quad 2\quad 3\quad 4\quad 5)^{-1}\\ &= (1\quad 2\quad 5\quad 3\quad 4)(5\quad 4\quad 3\quad 2\quad 1)\\ &= (1)(2\quad 4\quad 5)(3) = (2\quad 4\quad 5),\end{aligned}$$

故知此种情况 H 中必含 3 - 轮换.若 a 是两个对换的乘积,不妨设 $a = (1\quad 2)(3\quad 4)$, 取

$$\Sigma = (3\quad 4\quad 5) \in A_5,$$

计算得

$$H \ni \Sigma^{-1}a\Sigma = (5\ 4\ 3)(1\ 2)(3\ 4)(3\ 4\ 5) = (1\ 2)(4\quad 5),$$
$$H \ni \Sigma^{-1}a\Sigma \cdot a^{-1} = (1\ 2)(4\ 5)\cdot(1\ 2)(3\ 4) = (4\ 5\ 3).$$

即这时 H 也必含有 3 - 轮换.即(a)得证.

今证(b). 不妨设 $a=(1\quad 2\quad 3)$, 而去证任意 3 - 轮换 $(i_1\quad i_2\quad i_3)$ 与 a 在 A_5 中共轭. 令

$$\Sigma_1=\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ i_1 & i_2 & i_3 & j_1 & j_2\end{pmatrix},$$

$$\Sigma_2=\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ i_1 & i_2 & i_3 & j_2 & j_1\end{pmatrix}$$
$$=\Sigma_1\cdot(j_1\quad j_2),$$

易见 Σ_1,Σ_2 相差一个对换, 故一个是偶置换, 一个是奇置换. 不妨设其中的偶置换为 Σ 而计算

$$\Sigma^{-1}\cdot(1\quad 2\quad 3)\cdot\Sigma=(i_1,i_2,i_3),\quad \Sigma\in A_5,$$

故(b)得证. □

在上面证明中, 我们注意到 $n=5$ 而不是 $n=4$, 这很重要, 这提供给我们一个回旋余地, 使得能从容地选取满足我们需要的偶置换. 若 $n>5$, 即提供更多的回旋余地, 该是更能够作到, 即证明: $A_n, n>5$ 是单群. 但我们不在这里讨论而留给有兴趣的读者. 另一方面直接验证可知 A_4 不是单群.

下面讨论由行列式为 1 的二阶矩阵组成的特殊线性群 $SL_2(F)$, F 是数域. 显然 $\{\pm I\}, I=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$ 是它的中心. 常称商群 $PSL_2(F)=SL_2(F)/\{\pm I\}$ 为射影特殊线性群.

定理 9.5 数域 F 上的二阶射影特殊线性群 $PSL_2(F)$ 是单群.

证明 我们已知形如

$$\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix},\quad \begin{pmatrix}1 & 0\\ a & 1\end{pmatrix},\quad a\in F \tag{2}$$

组成 $SL_2(F)$ 的一个生成元集. 设 $H\neq\{\pm I\}$ 是 $SL_2(F)$ 的正规子群. 欲证定理, 只需证 $H=SL_2(F)$. 与上定理的证明步骤类似, 我们分三步去证:

(a) H 中包含一个上三角矩阵 $A\neq\pm I$.

(b) H 中包含一个形如 $\begin{pmatrix}1 & u\\ 0 & 1\end{pmatrix}$, $u\neq 0$ 的矩阵.

(c) H 中包含(2)中所有矩阵.

提醒一下, 在计算一个矩阵的共轭元素时我们只能用 $SL_2(F)$ 中的矩阵, 即行列式为 1 的矩阵.

(a)的证明 任取 H 中的一个矩阵 $A=\begin{pmatrix}a & b\\ c & d\end{pmatrix}$. 可设 $c\neq 0$, 否则已得

三角形矩阵.计算

$$PAP^{-1}=\begin{pmatrix}1&x\\0&1\end{pmatrix}\begin{pmatrix}a&b\\c&d\end{pmatrix}\begin{pmatrix}1&-x\\0&1\end{pmatrix}$$
$$=\begin{pmatrix}a+xc&*\\c&d-xc\end{pmatrix}=A'\in H,$$

选 x 使 $a+xc=0$，这样就在 H 中找到 $(1,1)$ 位置上为 0 的矩阵，仍记作 A，而设 $A=\begin{pmatrix}0&b\\c&d\end{pmatrix}$.

由于 $\det A=1$，故 $bc=-1$，取 $P=\begin{pmatrix}u&0\\0&u^{-1}\end{pmatrix}$ 而计算

$$P^{-1}A^{-1}PA=\begin{pmatrix}u&0\\0&u^{-1}\end{pmatrix}\begin{pmatrix}d&-b\\-c&0\end{pmatrix}\begin{pmatrix}u^{-1}&0\\0&u\end{pmatrix}\begin{pmatrix}0&b\\c&d\end{pmatrix}$$
$$=\begin{pmatrix}u^2&(1-u^2)bd\\0&u^{-2}\end{pmatrix}\in H.$$

如取 $u=2$，可知 $P^{-1}A^{-1}PA\neq\pm I$，而为所求者.

(b)的证明　由(a)，H 中含 $A=\begin{pmatrix}a&b\\0&d\end{pmatrix}\neq\pm I$. 若 $a\neq d$，取 $P=\begin{pmatrix}1&-1\\0&1\end{pmatrix}$ 而计算

$$H\ni P^{-1}A^{-1}PA=\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}d&-b\\0&a\end{pmatrix}\begin{pmatrix}1&-1\\0&1\end{pmatrix}\begin{pmatrix}a&b\\0&d\end{pmatrix}$$
$$=\begin{pmatrix}d&-d-b+a\\0&a\end{pmatrix}\begin{pmatrix}a&b\\0&d\end{pmatrix}=\begin{pmatrix}1&ad-d^2\\0&1\end{pmatrix},$$

此时 $ad-d^2\neq 0$，故上面矩阵即为所求.若 $a=d$，由于 $\det A=ad=1$，故或 $a=d=1$，此时 A 即为所求；或 $a=d=-1$，此时 A^2 即为所求.

(c)的证明　由(b)，H 中含 $\begin{pmatrix}1&u\\0&1\end{pmatrix}$，其中 $u\neq 0$ 是 F 中的一个特定数，先证 H 中必含所有的 $\begin{pmatrix}1&a\\0&1\end{pmatrix}$，其中 $a\in F$. 任取 $0\neq x\in F$，则

$$H\ni\begin{pmatrix}x&0\\0&x^{-1}\end{pmatrix}\begin{pmatrix}1&u\\0&1\end{pmatrix}\begin{pmatrix}x^{-1}&0\\0&x\end{pmatrix}=\begin{pmatrix}1&x^2u\\0&1\end{pmatrix}.\qquad(3)$$

另一方面，若 $\begin{pmatrix}1&x\\0&1\end{pmatrix},\begin{pmatrix}1&y\\0&1\end{pmatrix}\in H$，则其乘积 $\begin{pmatrix}1&x+y\\0&1\end{pmatrix}$ 及其逆 $\begin{pmatrix}1&-x\\0&1\end{pmatrix}$ 也在 H 中，这说明

$$K = \left\{ x \in F \middle| \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in H \right\}$$

是加群 $(F, +)$ 的一个子群. 由(3)知,对任意 $x, y \in F$, 有 x^2u, y^2u 以及 $x^2u - y^2u = (x^2 - y^2)u \in K$,但 F 中任何数都可表为 F 中某两个数 x, y 的平方差(只需取 $x + y = 1, x - y = b$ 就行了),故对任意 b, 有 $bu \in K$, 亦即 $K = F$. 这就说明了 H 中含所有 $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$, 其中 $a \in F$, 随之

$$H \ni \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -a & 1 \end{pmatrix}.$$

(c)得证. □

当 $n \geqslant 3$ 时 $PSL_n(F)$ 也是单群,这里我们略去证明.

当然 $PSL_2(F)$ 不是有限群,因为数域 F 含有无穷多个数,但如果有“有限域” F (这将在下一章讨论),则 $PSL_2(F)$ 将是一个有限群,在对“有限域” F 作某些小的限制,我们还知 $PSL_2(F)$ 是有限单群.

上面的证明中我们看到关于置换和矩阵的很巧妙的计算,数学中很多或者所有重大成果几乎都是把反映深刻本质的抽象概念和巧妙复杂的计算技巧结合起来的产物.

上面两个证明的计算中都出现 $xyx^{-1}y^{-1}$. 这是知道正规子群 H 中一个元素 y, 而想得到 H 中其他元素的第一个该用到的计算,因而它的一再出现不是偶然的. 常称之为 x, y 的换位子,容易看到 x, y 交换,即 $xy = yx$, 当且仅当其换位子为 e.

练习

1. 证明:当 $n \geqslant 3$ 时,对称群 S_n 中不存在 2 阶正规子群.
2. 设 $n \neq 4$. 证明:对称群 S_n 的正规子群只有 S_n, A_n 和 $\{(1)\}$.

§10 群的构造,自由群

群论研究可以分成两个侧面,一方面是对给定的有背景的重要群,如各种对象的对称群、置换群、矩阵群(和几何、物理的联系)、有限单群、可解群(与解代数方程有联系)等等,讨论群的结构,以及它与其他群的关系(群的表示问题). 另一方面是尽可能多地构造出一些新的群来,或者是借助于已知群去构造新群,或者就是根据需要去构造新群. 常称前者为群的结构理论和表示理

论，而称后者为群的构造理论．当然这两者是互相联系的．

前面我们讨论过的子群、商群，都是从一个已知群获得新群的方法．例如从一般线性群 $GL_2(F)$ 得到其子群 $SL_2(F)$，以及从 $SL_2(F)$ 得到 $PSL_2(F)$ 等等．

由两个已知群 K 和 H，依定义 8.5 由它们可以构造一个新的群，即它们的外直积 $H\times K$．

由已知的两个群 H 和 K，还可用别的方法构造新群吗？

一个我们非常感兴趣的问题是：能否构造一个群 G，它以 H 为正规子群（即它有一个正规子群与 H 同构）而它关于 H 的商群 $G/H\cong K$，即所谓群 H 借助于群 K 的扩张问题．这个问题的重要性我们已在有限单群在有限群论中起"基本构件"作用的讨论中看到过了．然而这个问题较专门，超出本课范围，就不在这里讨论了．

下面我们来构造自由群．

著名的 Cayley 定理说：一个 n 阶有限群可以看作是 n 元对称群 S_n 的一个子群．与此对偶地我们可以问：是否可找到一个群 G，使得某一类群中的所有群都是这个群 G 的同态象？如果这样的群 G 存在，那么研究这类群就归结为研究群 G 的商群，这就和研究有限群就是研究群 S_n 的子群有异曲同工之妙．

在前面曾说过，如果有满同态 $G\to G'$，则群 G 中的一些关系式（例如 $ab=ba$）必传递给 G'．这样上面我们想找的那个群 G，必是相当"自由"的群，即是关系很少的群．

这样的群我们已见过，加群 $\mathbb{Z}$ 和循环群之间就有这种关系：任一循环群都是群 $\mathbb{Z}$ 的同态象．下面首先来推广这一结果．

令 $\mathbb{Z}^n=\mathbb{Z}\times\mathbb{Z}\times\cdots\times\mathbb{Z}$（$n$ 个群 $\mathbb{Z}$ 的外直积）．这是一个交换群（其运算记作 $+$），n 元组 $\{e_1=(1,0,\cdots,0),e_2=(0,1,0,\cdots,0),\cdots,e_n=(0,\cdots,0,1)\}$ 是它的一个生成元集．

命题 10.1　任意由 n 个元素生成的交换群 G 都是 $\mathbb{Z}^n$ 的同态象．

证明　首先证明 $\mathbb{Z}^n$ 中每个元素可以唯一表示成

$$m_1e_1+\cdots+m_ne_n,\quad m_i\in\mathbb{Z}\tag{3}$$

的形式．任取 $a\in\mathbb{Z}^n$，则 $a=(m_1,m_2,\cdots,m_n)=(m_1,0,\cdots,0)+(0,m_2,0,\cdots,0)+\cdots+(0,\cdots,0,m_n)=m_1e_1+m_2e_2+\cdots+m_ne_n$，即 a 可表成(3)的形式．若

$$t_1e_1+t_2e_2+\cdots+t_ne_n=m_1e_1+m_2e_2+\cdots+m_ne_n,$$

则有

$$(0,\cdots,0)=(t_1-m_1)e_1+\cdots+(t_n-m_n)e_n$$

$$= (t_1 - m_1, \cdots, t_n - m_n),$$

即在群 $\mathbb{Z}$ 中有 $t_i - m_i = 0$. 即 $t_i = m_i$, $i = 1,2,\cdots,n$. 即得证表成(3)的形式时的唯一性.

再看由 n 个元素 $g_1,\cdots,g_n$ 生成的交换群 G (其运算也记作 +). 这时 G 的每一元素 g 都可表成某些 g_i, $-g_i$, $i = 1,\cdots,n$, 的和. 注意到 G 是交换群, 我们可以把同一足标的 g_i, $-g_i$ 调换到一起,这样就有

$$a = m_1 g_1 + m_2 g_2 + \cdots + m_n g_n, \quad m_i \in \mathbb{Z}, \tag{4}$$

即 G 中任一元 a 皆可表成(4)形式(由于对 g_i 无进一步了解,表成(4)形式时是否唯一就不得而知了).

规定

$$\begin{aligned} \phi: \quad & \mathbb{Z}^n \longrightarrow G \\ & m_1 e_1 + \cdots + m_n e_n \longmapsto m_1 g_1 + \cdots + m_n g_n. \end{aligned}$$

由于(3)形式的存在性和唯一性,得 ϕ 是一个映射. 由于(4)形式的存在性,得 ϕ 是满射. 至于 ϕ 保持运算,则很容易验证. 合起来就得 ϕ 是 $\mathbb{Z}$ 到 G 上的同态. □

也许直接用 $\mathbb{Z}^n$ 的元素的唯一表示形式 $(m_1,\cdots,m_n)$ 可以使上面证明短小一些. 但我们特别想看到 $\mathbb{Z}^n$ 的这组好生成元 $e_1,\cdots,e_n$.

上面的讨论使我们再一次感觉到有限生成的交换群和有限维向量空间的类似性:一个是数环 $\mathbb{Z}$ 上"向量空间",一个是数域上的向量空间. 这当然有很大差距,但还是有相似可类比的一些地方.

定义 10.2 称群 $\mathbb{Z}^n$ 为 n 阶自由交换群.

命题 10.1 说明: n 阶自由交换群 $\mathbb{Z}^n$ 在一定意义上"控制"了 n 个元素生成的交换群.

现在我们来构造能"控制"所有群的群,即所谓自由群.

这样群该是除了满足群的公理(结合律,有恒等元,有逆元)外不再有其它关系的群. 我们按照这个思路,从任意一组(有限或无限)符号 $X_1 = \{a,b,c,\cdots\}$ 出发,把这些符号 $a,b,c,\cdots$ 看成生成元而去构造一个群.

再取一组符号 $X_2 = \{a',b',c',\cdots\}$ (我们设想 a' 是 a 在将来要构造的群 G 中的逆元 a^{-1})而得 $X = X_1 \cup X_2 = \{a,b,c,\cdots,a',b',c',\cdots\}$, 称 X 中元素为字母. 任取 X 中有限多个字母,可以有重复的,把它们按某个次序排列起来,便算是一个 X - 字. 其长度规定为字母出现的次数(计重复数), 如 $bccc'b'bbb'a$, bca 是长度分别为 9 和 3 的 X - 字. X - 字 w 中的一个相连部

分称作 w 的子字,例如 bc 和 ccc' 都是上面第一个字的子字.我们特别引入长度为零的空字,记作 Λ. 而令 W 表示所有 X - 字及空字 Λ 的全体.

任取一个长为 n 的 X - 字 w,若 w 有形如 aa' 或 $a'a$ 的子字,我们把它拿掉而得一长为 $n-2$ 的 X - 字.例如上面第一个字中拿掉 cc',便得字 $bcb'bbb'a$.重复这个步骤继续作下去或者得到空字,或者得到一个不含形如 aa', $a'a$ 子字的 X - 字 w_1. 这时我们称 X - 字 w_1 或空字 Λ 或为字 w 的既约形式.这个"拿掉"过程不是唯一的,因而 w 的既约形式是否是唯一的便是个问题了,先看一个例子

$$\begin{array}{ccc}
ba\,\underline{b'b}a'c'cac' & \qquad & bab'ba'\underline{c'c}ac' \\
\downarrow & & \downarrow \\
b\,\underline{aa'}c'cac' & & ba\,\underline{b'b}a'ac' \\
\downarrow & & \downarrow \\
b\,\underline{c'c}ac' & & ba\,\underline{a'a}c' \\
\downarrow & & \downarrow \\
bac' & & bac'
\end{array}$$

拿掉过程的确不同,但可喜的是结果相同.我们的直觉是一般情况这也是对的.但把直觉变成一个令人信服的说法,常不是一件容易的事.下面命题读者可以承认下来而略其证明,也可以看看人家是怎样巧妙地把直觉变成一个说法的.

约定:经过一系列"拿掉"而把字 w 化成既约形式的过程,称为一个简约过程.

命题 10.3 任何一个 X - 字 w 都有唯一的既约形式.

证明 对字长作数学归纳法,令 w 之长为 n 而假定其长小于 n 的任意字都有唯一的既约形式.

若 w 本身就是既约形式,就没什么可证了.今设 w 不是既约形式,不失一般性,可认定

$$w = \cdots \underline{aa'} \cdots \tag{5}$$

先看以拿掉上面标出这对字母 aa' 为第一步的简约过程(简记作 $\sum$).对这些简约过程,第一步拿掉这个 aa' 后,便得同一个字 w_1,它的长小于 n,依归纳假设,无论再采取什么简约过程,w_1 都化到相同的既约形式,这样,w 经过这些过程 $\sum$ 化到同一既约形式.

下面的讨论想说明,字 w 的任意一个简约过程 θ 都相当于对 w 施行一个简约过程 $\sum$,分两种情形讨论.

(a) 在简约过程 θ 的第 k 步拿掉(5)中标出的这对字母 aa'. 这就是说

在前 $k-1$ 步中(5)中标出的 aa' 未被触动,这时我们把拿掉(5)中 aa' 当作第一步,其余再按 θ 去作.这样,我们得到一个简约过程 $\sum$.易见 w 分别经过 θ 和 $\sum$ 的前 k 步后便化到同一个字 w_k,而从 $k+1$ 步起过程 θ 和过程 $\sum$ 是完全一样的.这就证明施行 θ 和施行 $\sum$ 是一样的.

(b) 在整个简约过程 θ 中始终没有一步是拿掉(5)中 aa' 的.但显然它们不能保留在最后既约形式中,故必在某一步,说是第 k 步,拿掉了(5)中 a 或 a',这就是说 θ 的第 k 步必是下面两种情形之一,

$$\cdots a'\underline{aa'}\cdots \quad 或 \quad \cdots \underline{aa'}a\cdots$$

但这和在第 k 步拿掉(5)中标出的 aa' 的效果是完全一样的.这样这种情形就归结为情形(a)了.□

令 $F=\{$所有具有既约形式的 $X-$字,空字 $\Lambda\}$,任取 F 中两个元素 w_1, w_2,把它们并写在一起便得 $X-$字 w_1w_2,但它可能不具既约形式.用 $[w_1w_2]$ 表示 w_1w_2 唯一既约形式,而规定 F 的运算为:

$$w_1\cdot w_2=[w_1w_2].$$

今证

定理 10.4 $(F,\cdot)$ 是一个群.

证明 (a) 结合律.设 $w_1,w_2,w_3\in F$,则

$$(w_1\cdot w_2)\cdot w_3=[[w_1w_2]w_3],$$
$$w_1\cdot(w_2\cdot w_3)=[w_1[w_2w_3]].$$

易见两等式右侧的既约形式都等于 $X-$字 $w_1w_2w_3$ 的既约形式,这是因为第一个是先在 $w_1w_2w_3$ 的 w_1w_2 部分上简约,而第二个是先在 $w_1w_2w_3$ 的 w_2w_3 部分上简约,而由命题 10.3,一个字的既约形式是和简约过程没有关系的.

(b) 易见空字 Λ 是恒等元.

(c) 若 $w\in G$, $w=xy\cdots z$ 具有既约形式,其中,例如 x 是 a 或 a',约定当 $x=a$ 时 $x'=a'$ 而当 $x=a'$ 时 $x'=a$.作 $w'=z'\cdots y'x'$,则知 w' 也具有既约形式,即 $w'\in F$ 且

$$w'\cdot w=[z'\cdots y'x'xy\cdots z]=\Lambda,$$
$$w\cdot w'=[xy\cdots zz'\cdots y'x']=\Lambda,$$

即定理得证.□

易见群 $(F,\cdot)$ 以 $X_1=\{a,b,c,\cdots\}$ 为生成元集,而其中 $a'=a^{-1}$, $b'=b^{-1}$,等等.以后我们将把 F 中的 a', b' 等直接写成 a^{-1}, b^{-1} 等.

定义 10.5 称 $(F,\cdot)$ 为自由群. 称 $X_1=\{a,b,c,\cdots\}$ 为自由群 F 的自由生成元集.

定理 10.6 任意群 G 都同构于一个自由群 F 的商群.

证明 任取群 G 的一个生成元集 $A=\{g_i,i\in I\}$. 这总是存在的,至少 $A=G$ 是 G 的生成元集. 相应地取 $X=\{x_i,i\in I\}$,而令以 X 为自由生成元集的自由群为 F. 由自由群的定义知 F 中的元素可唯一地写成既约形式 $y_{i_1}y_{i_2}\cdots y_{i_m}$,其中 y_{i_j} 是 x_{i_j} 或 $x_{i_j}^{-1}$,我们规定映射

$$\begin{aligned}\phi:\quad F &\longrightarrow G\\ y_{i_1}\cdots y_{i_m} &\longmapsto h_{i_1}\cdots h_{i_m},\end{aligned}$$

其中

$$h_i=\begin{cases}g_i, & \text{若 } y_i=x_i;\\ g_i^{-1}, & \text{若 } y_i=x_i^{-1}.\end{cases}$$

易见 $\phi(x_i)=g_i,\phi(x_i^{-1})=g_i^{-1}$,而实际上 ϕ 的实质就是先让 $x_i\longmapsto g_i$,$x_i^{-1}\longmapsto g_i^{-1}$ 然后再把它扩张到既约形式 $y_{i_1}\cdots y_{i_m}$ 上去. 由于 F 中元素唯一表成既约形式,故 ϕ 是一个映射,由于 G 中元素表成某些生成元及其逆的乘积(这当然不是唯一的)时,总可选定一种形式,其中不出现 $g_ig_i^{-1}$ 或 $g_i^{-1}g_i$,因而把此乘积中 $g_i(g_i^{-1})$ 换成 $x_i(x_i^{-1})$ 时便得到一个具有既约形式的 X - 字,即 F 中元素,故知 ϕ 还是满射. 至于 ϕ 保持运算则是显然的,即得 ϕ 是 F 到 G 上的同态. □

这样,对任意群 G,都有 $G\cong F/H$,F 是自由群,H 是 F 的正规子群,从而给出了一个构造具有给定关系的群的办法.

由于一个群 F 中的一些(有限或无限个)正规子群之交仍是正规子群,给定 F 的一个子集 S 必有一个含 S 的最小正规子群 H,称 H 为 S 在群 F 中生成的正规子群,记作 $H=(S)$.

设 F 是自由群,$X=\{a,b,c,\cdots\}$ 是 F 的自由生成元集. 任取 F 的一个子集,即由一些具既约形式的 X - 字组成的 $S=\{w,u,v,\cdots\}$,令 $H=(S)$ 而得 $G=F/H$. 此时我们称群 G 是由 X 和 S 所定义的,并表成 $G=<X;\delta>$,其中 X 称为群 G 的生成元集,S 称为群 G 的关系集,w,u,v 等称为定义关系式.

若 $G=F/H$,而一个 X - 字,例如说是,$aabca^{-1}b^{-1}\in H$,则在 G 中显然有关系式

$$aabca^{-1}b^{-1}=e \quad (G \text{ 的恒等元}).$$

这时我们自然称 $aabca^{-1}b^{-1}$ 为群 G 的一个关系. 这样正规子群 H 中的元素都是群 G 的关系. 另一方面,若对 X - 字 r,$r=e$ 是群 G 的关系式,则显然 r

$\in H$. 我们当然愿意知道最基本的关系，亦即其他关系可由它们推出. 若 $H = (S)$，则 S 就是一个基本关系集，因为 H 中元素可通过 S 中元素，及其共轭元素以及它们的逆元的乘积来表示. 正规子群的生成元集当然不是唯一的，因而群 G 的基本关系集也不是唯一的.

如果我们希望有一个有限生成的群，其中任一元素的 n 次幂都等于 e，n 是一个固定的正整数，就可取 $G = \langle x_1, \cdots, x_m; [w^n] \mid w$ 是任意 X - 字 $\rangle$. 著名的限制 Burnside 问题是问：这个群 G，即一个有限生成，而元素的阶有界的群是否是有限的. 这个问题是已肯定地解决了，而 Burnside 问题，即问一个有限生成的周期群(即每个元素的阶是有限的)是否为有限的，则是否定地解决的.

在第二章讨论一个群的生成元集，以及关于此生成元之间的一些关系时，曾留有一个问题：怎样知道这些关系是完全的，即这组生成元之间的其他关系都可由它们推出来. 利用自由群的概念，可在原则上回答这一问题.

设群 G 有生成元集 $A = \{g_i, i \in I\}$，以及关于这个生成元集 A 的一些关系，这就是由一些 A - 字 $\bar{w}, \bar{u}, \bar{v}, \cdots$ 组成的集 $\bar{S} = \{\bar{w}, \bar{u}, \bar{v}, \cdots\}$. 相应于集 A 我们取自由生成元集 $X = \{x_i, i \in I\}$，相应于 A - 字 $\bar{w}, \bar{u}, \bar{v}, \cdots$ 我们得 X - 字 $w, u, v, \cdots$，而得 $S = \{w, u, v, \cdots\}$. 令 F 是以 X 为自由生成元集的自由群，而 $H = (S)$. 依定理 10.6，我们有满同态 $\phi: F \to G$. 令 $\mathrm{Ker}\phi = K$. 由于 $\phi(w) = \bar{w} = e, \phi(u) = \bar{u} = e, \cdots$，知 w, u, v 等属于 K，即 $S \subseteq K$，随之 $H = (S) \subseteq K$. 一般言，H 较 K 集小，若是 $H = K = \mathrm{Ker}\phi$，即是有 $F/H \cong G$，亦即 G 同构于一个以 X (它相应于 A)为生成元集和以 S (它相应于 $\bar{S}$)为定义关系集的群. 这当然就说明了关系集 $\bar{S}$ 是完全的.

例 1 二面体群 D_4 以 $a = \rho_\theta, \theta = 2\pi/4$，及 $b = r$ 为生成元. 我们已知 a, b 满足关系式：$a^4 = 1, b^2 = 1, abab = 1$. 为了看一下这组关系式是否完全，取自由生成元 x, y，而作自由群 F. 令 $H = (x^4, y^2, xyxy)$，由定理 10.6 有满同态 $\phi: F/H \to D_4$. 现在考察是否有 $F/H \cong D_4$. 在前面我们已经知道 D_4 的阶是 8，今计算 $\bar{F} = F/H$ 共有多少元素.

在群 $\bar{F}$ 中，显然有关系式 $\bar{x}^4 = e, \bar{y}^2 = e, \overline{xyxy} = e$，利用这些关系易知每一 $\{\bar{x}, \bar{y}\}$ - 字都可化归为 $\bar{x}^i, \bar{x}^i\bar{y}, 0 \leqslant i \leqslant 3$ 的形状，即 $\bar{F}$ 最多有 8 个元素. $\bar{F}$ 的元素当然不会少于 8，故得 $\bar{F}$ 恰有 8 个元素，ϕ 是一一对应，因而 $F/H \cong D_4$. 这就说明了我们找到的 D_4 的生成元 a, b 的关系式是完全的.

下面我们简单介绍一下自由半群. 它在半群论中起的作用和自由群在群

论中起的作用类似.因为不像群中要求有逆元,随之没有相消的问题,自由半群的定义就容易多了.

任取一组符号 $X = \{a, b, c, \cdots\}$,而集 $S = \{$ 空字 Λ,以及所有 X - 字$\}$.在集 S 中引入运算:若 w, u 是两个 X - 字,则规定 $w \cdot u = wu$,即 w 和 u 的乘积就规定为把 w, u 连结在一起而成的 X - 字 wu.容易证明,这个乘法满足结合律,而空字 Λ 起恒等元的作用,即 $\Lambda \cdot w = w = w \cdot \Lambda$,对每一个 X - 字 w.这样 $(S, \cdot)$ 便是一个带恒等元的半群,称 S 为幺自由半群,而 X 为它的自由生成元集.

设 S 如上,在集 S 中引入一个关系 $\sim$: $w \sim u$ 当且仅当 X 中每一符号在 X - 字 w 和 X - 字 u 中出现(不计次序)的次数一样多.例如 $abaab \sim babaa$.这是集 S 的一个等价关系,并且若 $w \sim u, w' \sim u'$,显然有 $ww' \sim uu'$,即 $\sim$ 还是半群 S 的一个合同关系.这样把关于 $\sim$ 的等价类作为元素看,令这些等价类的全体为 $\overline{S}$.令 w 所在的等价类记作 $[w]$,而规定 $\overline{S}$ 的运算 $\cdot$ 如下:

$$[w] \cdot [u] = [wu].$$

由于 $\sim$ 是半群 S 的一个合同关系,上面定义与代表选择无关,即若 $[w] = [w'], [u] = [u']$,可得 $[w] \cdot [u] = [wu] = [w'u'] = [w'] \cdot [u']$.易见 $(\overline{S}, \cdot)$ 作成一个半群.

由于对任二 X - 字 w, u,在 X - 字 wu 和 X - 字 uw 中出现每一符号的次数一般多,故 $wu \sim uw$,即 $[wu] = [uw]$,这就是说

$$[w] \cdot [u] = [wu] = [uw] = [u] \cdot [w],$$

即 $\overline{S}$ 是交换半群,$[\Lambda]$ 仍是它的恒等元.我们称 $\overline{S}$ 为幺自由交换半群,而 $\overline{X} = \{[a], [b], [c], \cdots\}$ 为它的自由生成元集.

你感兴趣的话,可以试着定义半群 A 到半群 B 的同态映射,然后你就可试着去证,任意半群都是某一个自由半群的同态象,而任意交换半群都是某一个自由交换半群的同态象.不过我们在此略去这些讨论.

练习

1. 设 G 是由元素 a, b 生成的群,其中 a, b 的定义关系为 $a^2 = b^3 = e$ 和 $(ab)^3 = e$.写出 G 中元素并证明:G 与交代群 A_4 同构.

2. 设 G 是由元素 a, b 生成的群,其定义关系为 $a^2 = b^3 = e$ 和 $ab = b^2a$.又设 $\overline{G}$ 是由元素 x, y 生成的群,其定义关系为 $x^2 = y^2 = (yx)^3 = e$.证明:G 与 $\overline{G}$ 是群同构.

§11 群在集上的作用

在我们把变换群等具体群概括成抽象群的概念时,有一个侧面我们忽略

了，这就是这些变换群总是作用在一个集合上的.具体说，设 S 是集 M 上的变换群 $T(M)$ 的一个子群，则任取 $s \in S$，s 总是集 M 到 M 上的一个一一变换，即对任意 $x \in M$，我们有 $s(x) \in M$. 如果把它解释为 $S \times M$ 到 M 的一个运算，也就是令 $s \cdot x = s(x)$，这个运算显然满足下列条件

A1) 对任意 $s, h \in S, x \in M$，有 $s \cdot (h \cdot x) = sh \cdot x$.

A2) 对任意 $x \in M$，e 是 S 的恒等元，有 $e \cdot x = x$.

现在我们把变换群 $S \subseteq T(M)$ 作用在集 M 上的概念，引到抽象群论中来.

定义 11.1 设 G 是一个任意群，M 是一个集合，设 $\times$ 是 $G \times M$ 到 M 的一个运算(映射)，即对任意 $g \in G, x \in M$，有 $g \times x \in M$，如果运算 $\times$ 满足条件：

A1) 对任意 $g, h \in G, x \in M$，有 $g \times (h \times x) = gh \times x$.

A2) 对任意 $x \in M$，e 是群 G 的恒等元，有 $e \times x = x$.

则称 M 为一个左 G －集.此时也说 $\times$ 给出群 G 在集 M 上的一个作用.当不会引起混淆时常简称之为群 G 作用在集 M 上.

“左”字是强调群 G 是从左侧作用到集 M 上.类似地可定义右 G －集.

显然，变换群 $S \subseteq T(M)$，依上定义，作用在集 M 上.

设 M 是一个左 G －集，任取 $g \in G$，可利用之定义

$$t_g:\quad M \longrightarrow M$$
$$x \longmapsto g \times x.$$

当 $g = e$ 时，易见 t_e 是 M 的恒等变换.由于对任意 $h, g \in G$，$x \in M$ 有

$$(t_g t_h)(x) = t_g(t_h(x)) = t_g(h \times x)$$
$$= g \times (h \times x) = gh \times x = t_{gh}(x),$$

得 $t_g t_h = t_{gh}$. 特别，我们有 $t_g t_{g^{-1}} = t_{g^{-1}} t_g = t_e = M$ 的恒等变换，由之得每一 t_g 都是集 M 的一个一一变换，即 $t_g \in T(M)$. 作映射

$$\phi:\quad G \longrightarrow T(M)$$
$$g \longmapsto t_g.$$

上面的讨论说明 ϕ 是群 G 到变换群 $T(M)$ 中的一个同态对应.这就是说，知道一个 G －集，便可得群 G 到一个变换群的同态.

反过来，已知同态对应 $\phi: G \to T(M)$. 这时 G 中元素 g 在 ϕ 下的象 $\phi(g) = t_g$ 是集 M 的一个一一变换.如果我们规定 g 对集 M 的作用就是 t_g 在 M 上的作用，亦即规定：

$$g \times x = \phi(g)(x) = t_g(x),$$

可以想象这时 M 该是一个左 G －集，实际上也确是如此，即有

$$g \times (h \times x) = g \times (t_h(x)) = t_g(t_h(x)) = (t_g t_h)(x)$$
$$= t_{gh}(x) = gh \times x.$$

这就证得 A1).上式的推导中,除 $t_g t_h = t_{gh}$ 是用到已知条件:ϕ 是同态对应外,其余每一步都是按照定义推出的.A2)之成立则由于 $\phi(e) = t_e$ 是 $T(M)$ 的恒等元,亦即是集 M 的恒等变换.这就是说,知道一个群 G 到变换群的一个同态,便可得到一个左 G - 集.

总结一下就是,寻找群 G 到变换群的同态对应(这也就是群 G 的变换群表示问题)和寻找 G - 集是一回事. G - 集似乎比群 G 到变换群的同态更容易掌握一些.

在具体群类中,集合的变换群和向量空间的线性变换群占有特别重要的地位.任意群 G 和变换群(或线性变换群)的同态关系,就是 G 的变换群(或线性变换群)表示问题.特别是群 G 的线性变换群(即矩阵群)表示问题,是群论中很重要、很感兴趣的问题.上面我们把前者归结为寻找 G - 集的问题,用的方法是把变换群对集合的作用推广成抽象群 G 对集合的作用.如果把线性变换群对向量空间的作用,推广成抽象群 G 对向量空间的作用,你该能得到"G - 向量空间"的概念,随之,仿上,你该也能把寻找群 G 的线性变换群表示问题(由于它的重要性常称为群的表示理论)归结为寻找 G - 向量空间的问题.

下面我们来寻找 G - 集. G - 集 M,或者群 G 和变换群 $T(M)$ 的同态,都是群 G 与 G 的外部世界的联系.下面将看到, G - 集 M 完全由群 G 的内部结构所确定.

先看看利用群 G 本身可以作出一些什么 G - 集来.

G 本身就是一个 G - 集,为此只需定义群 G 在集 G 上的作用为:对任意 $g, x \in G$,有 $g \times x = gx$. 容易验证,在此定义下,我们得到一个 G - 集 G. 其实在前面证明群 G 必同构于变换群 $T(G)$ 的子群时,已经用过这个 G - 集 G.

设 H 是群 G 的一个子群,考察 H 的所有左陪集组成的集合 $G/H = \{xH \mid x \in G\}$. 这时因为 H 不一定是正规子群, G/H 一般不作成一个群,而只是集 G 的一个商集.规定群 G 在集 G/H 上的作用为: $g \times xH = gxH$, 容易验证,A1),A2)成立,而使我们得到一个 G - 集 G/H. 取 $H = \{e\}$, 便得到上面讨论过的 G - 集 G.

这样对每一子群 H(无论是正规子群,或非正规子群),我们都有 G - 集 G/H. 这些就是从 G 本身所获得的 G - 集.

下面我们来看看,任给的一个 G - 集 M 是什么样子.

为简化符号将把 $g \times m$ 记作 gm. 这样 A1)就是 $g(hm) = (gh)m$, 而 A2)就是 $em = m$. 只要弄清是对哪两个元素进行运算,便会知道该运算是群中的运算还是群 G 对集 M 的作用,而不会引起混淆.

在集 M 中引入一个传递关系,说 M 中 x, y 有传递关系,记作 $x \sim y$, 如果存在 $g \in G$ 使 $gx = y$. 传递关系是一个等价关系,这是因为由 $ex = x$ 得 $x \sim x$, 若 $gx = y$ 则 $g^{-1}y = g^{-1}(gx) = (g^{-1}g)x = ex = x$, 即有:若 $x \sim y$ 必有 $y \sim x$, 类似地可得传递律.

任取 $x \in M$, 在传递关系下 x 所在的等价类设为 O_x. 易见 $O_x = \{gx, g \in G\}$. 从几何的角度去看, O_x 即 x 在群 G 作用下所走的轨迹,今后特称之为 x 所在的 G - 轨道,常略去 G 而称之为轨道. 例如,我们在讨论有限运动群的分类时曾用过 O_x (命题 4.1 的证明). 又例如,如果取 $G = (\rho_\theta, \theta = 2\pi/n)$, 取 x 为单位圆周上一点,则 O_x 为单位圆周上一组 n 等分点,若取 y 为原点,则 O_y 只由这个原点组成. 这样 M 被划分为 M 中一些不相交的轨道之并:

$$M = \bigcup_x O_x. \tag{1}$$

如果我们了解每一个轨道的情况,则整个 G - 集 M 也就在掌握之中了.

定义 11.2　设 M 为 G - 集.

(a) 称 $O_x = \{gx \mid g \in G\}$ 为 M 中点(元素) x 所在的 G - 轨道.

(b) 若 G - 集 M 只有一个 G - 轨道,即对任意 $x \in M$, 有 $M = O_x$, 也就是说, M 中任意两个元素 x, y 总有关系: $y = gx, g \in G$, 则称 M 为传递 G - 集.

(c) 称 $S_x = \{g \in G \mid gx = x\}$ 为 M 中元素 x 的对称群(或稳定群).

对(c)作一些说明. S_x 确是群 G 的一个子群,这是因为,若 $g_1, g_2 \in S_x$, 则由 $(g_1g_2)x = g_1(g_2x) = g_1x = x$, 以及 $g_1^{-1}x = g_1^{-1}(g_1x) = ex = x$ 知 g_1g_2 及 g_1^{-1} 也在 S_x 中,故 S_x 是子群. 如果用 M 的一个子集 N 来代替 x, 则可考虑集

$$S_N = \{g \in G \mid gN = N\} \subseteq G,$$

其中 $gN = \{gx \mid x \in N\}$. 同样可证明 S_N 是 G 的一个子群,可称之为 N 的对称群. 例如,若取 G 为平面运动群, N 取为一个平面图形上的点集,则 S_N 就是平面图形 N 的对称群,这样我们顺便也就把具体直观的图形的对称群的想法抽象到一般群 G 和 G - 集 M 上来,而使得抽象的 G - 集的讨论有一个具体的几何背景.

这些抽象对称群 S_x, S_N 是很重要而有用的,许多群常是作为 $S_x(S_N)$ 而出现的. 现在则来给出传递 G - 集的结构定理.

定义 11.3 设 G 是群，M, M' 是 G - 集，若 ϕ 是集 M 到 M' 上的一个一一映射，且满足对任意 $g \in G$ 和 $m \in M$，有 $\phi(gm) = g\phi(m)$，则称 ϕ 是 G - 集 M 到 G - 集 M' 上的同构对应. 此时称 G 集 M 同构于 G - 集 M'.

定理 11.4 设 M 是传递 G - 集，则有群 G 的子群 H，使得 G - 集 M 同构于 G - 集 G/H.

证明 任取定 $m \in M$，而令 $H = S_m$. 规定

$$\begin{aligned} \phi:\quad G/H &\longrightarrow M \\ gH &\longmapsto gm. \end{aligned}$$

首先证明 ϕ 是一个映射，即需证：若 $g_1H = g_2H$，则 $g_1m = g_2m$，这样 gH 的象 gm 与所用代表元素 g 的选择无关，因而是唯一确定的. 由 $g_1H = g_2H$，得 $g_1 = g_2h, h \in H$. 此时注意到 $hm = m$（这是由 $H = S_m$ 的定义），便有 $g_1m = (g_2h)m = g_2(hm) = g_2m$.

再证 ϕ 是单射. 设 $gH \longmapsto gm, g'H \longmapsto g'm$ 且 $gm = g'm$ 则有 $(g^{-1}g')m = g^{-1}(g'm) = g^{-1}(gm) = m$，依 S_m 的定义知 $g^{-1}g' \in S_m = H$，即 $g' \in gH$，随之 $g'H = gH$，即证得 ϕ 是单射. 由 M 是传递 G - 集，即任意 $x \in M$ 都可写成形式 $x = gm$，故知 ϕ 是满射.

最后来证 ϕ 是保持运算的. 对任意 $f, g \in G$ 我们有

$$\phi(f \times gH) = \phi((fg)H) = (fg)m = f(gm) = f\phi(gH),$$

即得证 ϕ 是 G - 集 H/G 到 G - 集 M 上的同构对应. □

在上面证明中我们是任取 $m \in M$，而令 $H = S_m$，如果取 M 中的另一元素，比如说是 gm，则 S_{gm} 会是另外一个子群 H'. 注意到 $gS_mg^{-1}(gm) = gm$，由之可以得到

$$S_{gm} = gS_mg^{-1}.$$

这就是说，在传递 G - 集中，不同点的对称群可以不相同，但它们是彼此共轭的.

上定理和(1)合在一起说明，只要我们能找出群 G 的所有子群 H 来，我们就能构造所有可能的 G - 集，因而得出群 G 和所有变换群的所有可能的同态关系.

当 G - 集 M 是有限集时(1)还给出下面计数公式：M 中元素个数等于各轨道的元素个数之和，即

$$|M| = \sum_x |O_x|. \tag{2}$$

这是一个有很多应用的计数公式. 不过在此我们不做进一步的讨论，只是用 G - 集的语言，即轨道和对称群 S_x 的语言再解释一下我们已经知道的事情.

例 1 G 是一个群，这一次用另外一种方式来定义 G - 集 G：$g \times x =$

$gxg^{-1}, g, x \in G$. 即规定 g 在集 G 上的作用为 g 所决定的内自同构 T_g 在集 G 上的作用. 容易验证, 这使得集 G 成 G - 集. 此时 O_x 就是 x 所在的共轭元素类. 当 G 有限时, 公式(2)就是: 群 G 的阶等于各共轭元素类的元素个数之和. 这个事实我们曾经得到过.

例 2 G 是一个群而 H 是它的子群, 如下可把集 G 定义为 H - 集: 规定 $h \times x = hx, h \in H, x \in G$. 此时 $O_g = \{hg | h \in H\} = Hg$. 当 G 为有限时, 公式(2)就是: 群 G 的阶等于各右陪集 Hg 的元素个数的和, 这也就是群 G 的阶等于子群 H 的阶乘以子群 H 在群 G 中的指数.

例 3 设 $G = GL_n(F)$, F 是数域.

1) 令 M 为所有 F 上 $n \times n$ 矩阵所作成集合. 按下方式把 M 定义为 G - 集: $P \times A = PAP^{-1}, P \in G, A \in M$. 这确是 G - 集, 除显然有 $E \times A = EAE^{-1} = A$ (E 是单位矩阵), 我们还有: 当 $P, H \in G, A \in M$,

$$\begin{aligned} P \times (H \times A) &= P \times (HAH^{-1}) = PHAH^{-1}P^{-1} \\ &= (PH)A(PH)^{-1} = PH \times A. \end{aligned}$$

线性代数中说两个矩阵相似就等价于这里说该两矩阵属于同一轨道, 而当 $F = \mathbb{C}$ 时, A 的 Jordan 标准型就是 A 所在轨道中的最佳代表.

(2) 令 N 是 F 上所有 $n \times n$ 对称矩阵的集合. 把 N 定义为 G - 集(留给读者去验证): $P \times A = PAP^T$, P^T 是 P 的转置矩阵, $P \in G, A \in N$. 线性代数中说两个对称矩阵等价就等于说该两矩阵在此 G - 集的同在一轨道中. 当 $F = \mathbb{R}$ 时, Sylvester 指标定理是说在此 G - 集的每一轨道中有一标准代表

$$E_{r,s} = \begin{pmatrix} 1 & & & & & & & & \\ & \ddots & & & & & & & \\ & & 1 & & & & & & \\ & & & -1 & & & & & \\ & & & & \ddots & & & & \\ & & & & & -1 & & & \\ & & & & & & 0 & & \\ & & & & & & & \ddots & \\ & & & & & & & & 0 \end{pmatrix},$$

其中 r 表示其中 1 的个数而 s 表示 -1 的个数.

当 $F = \mathbb{R}$ 时, 单位矩阵 E 的对称群 $S_E = \{P \in GL_n(\mathbb{R}) | PP^T = E\}$ 就是 n 维正交群, 即保持正定二次型 $x_1^2 + x_2^2 + \cdots + x_n^2$ 不变的线性变换组成的正交群.

如果取 $n = 4$, 而令

$$A=\begin{pmatrix}1&&&\\&1&&\\&&1&\\&&&-1\end{pmatrix}=E$$

则矩阵 A 的对称群 $S_A=\{P\in GL_4(\mathbb{R})\mid PAP^T=A\}$ 是物理中4维时空空间的著名的 Lorentz 群,也就是保持不定二次型 $x^2+y^2+z^2-t^2$ 不变的线性变换组成的矩阵群,在规范化的意义下,这也就是保持 $x^2+y^2+z^2-c^2t^2$(这里 c 表示光速)不变的4维时空空间的线性变换群,后者的意义是保持光速不变的线性变换群.

例 4 设 G 是一个有限群,其阶 $n=p^tm$,其中 p 是素数,设 M 是集 G 中元素个数为 p^t 的子集的全体,今定义

$$g\times A=gA,\quad g\in G,A\in M,$$

由于 gA 所含元素个数和 A 一样多,故 gA 也是 M 中的元素.直接验证可知这个群 G 到集 M 上的作用使得 M 成为一个 G - 集.用一个很有技巧的办法可以证明(略去):存在 M 中的一个元素 A,使得 A 的对称群 S_A 就是群 G 的元素个数为 p^t 的子群,特别,当 p,m 互素时,S_A 就是群 G 的 Sylow p - 子群.

练习

1. 设 G 是群、M 是 G 的子群全体的集合.定义 G - 集 M:对任意 $g\in G$ 和 $H\in M$,规定 $g\times H=gHg^{-1}$.

 1)说明上述定义了群 G 在集合 M 上的作用.

 2)证明:$H\in M$ 是 G 的正规子群当且仅当 H 的对称群 $S_H=G$.

2. 设 G 是有限群,m 是正整数且 $m\leqslant|G|$,设 M 是集 G 中元素个数为 m 的子集全体的集合.对任意 $g\in G$ 和 $A\in M$,定义 $g\times A=gA$.

 1)说明上述定义了群 G 在集 M 上的作用.

 2)对任意 $A\in M$,记 S_A 是 A 的对称群,证明:$|S_A|\mid m$.

本章习题

1. 设 G 是群.$a\in G$,任取两自然数 s,t.证明:

 1)$\langle a^s\rangle\cap\langle a^t\rangle=\langle a^{[s,t]}\rangle$;

 2)$\langle a^s\rangle\cdot\langle a^t\rangle=\langle a^{(s,t)}\rangle$.

这里 $[s,t]$ 是 s,t 的最小公倍数,(s,t) 是 s,t 的最大公约数.

2. 如果 G 中每个元的阶都小于或等于2.证明:G 是交换群.

3. 设 H 是群 G 的子群,且 H 含于 G 的中心,如果商群 G/H 是循环群.证明:G 是交换群.

4. 证明:阶为 p^2 (p 为素数)的群为交换群.

5. 设 G 是交换群,且 $|G| = p_1p_2\cdots p_t$,其中 $p_1,\cdots,p_t$ 是两两不同的素数. 证明: G 是循环群.

6. 设 S 是 G 的真子群,证明 $G \neq \bigcup_{g\in G} gSg^{-1}$.

7. 设 A,B 是群 G 的两个有限子群,证明 $|AB| = \dfrac{|A|\cdot|B|}{|A\cap B|}$.

8. 设 K,H 是群 G 的两个子群,且 $H\subseteq K$,如果 $[G:H]$ 有限,证明: $[G:H] = [G:K][K:H]$.

9. 设 A,B 是群 G 的两个指数有限的子群,证明 $[G:A\cap B]\leqslant[G:A][G:B]$,且等号成立当且仅当 $G = AB = BA$.

10. 设 $G = \langle a\rangle$ 是 n 阶循环群,求 $\mathrm{Aut}(G)$.

11. 设 G 是群,证明有群同构 $G/C\cong \mathrm{Inn}(G)$,其中 C 是 G 的中心.

12. 设 H 是群 G 的子群,记 $M = \{Hg \mid g\in G\}$ 和 $T(M)$ 是 M 上全体变换在合成下形成的群(此时记变换的作用在右边). 对任意 $a\in G$,定义: $\tau_a: M\to M,\quad Hg\longmapsto Hga$. 证明:

1)对任意 $a,b\in G$,τ_a 是 M 上的一个变换. 且 $\tau_a\tau_b = \tau_{ab}$;

2)如果定义 $\phi: G\to T(M),\quad a\longmapsto \tau_a$,那么 ϕ 是群同态且 $\mathrm{Ker}\phi = \bigcap_{g\in G} g^{-1}Hg$.

13. 设 H 是群 G 的子群,且 $[G:H] = n$,证明:存在 G 的正规子群 K,使得 $K\subseteq H$ 且 $[G:K]\mid n!$.

14. 设 G 是有限单群且非交换,设 p 是 $|G|$ 的最小素因数. 证明:不存在 G 的子群 H,使得 $[G:H] = p$.

15. 设 $n>2$. 证明:对称群 S_n 的中心 C 平凡,即 $C = \{e\}$.

16. 设 $\tau = (i_1,\cdots,i_t)$ 是 S_n 的一个 t-轮换,证明: τ 是奇置换当且仅当 t 为偶数.

17. 设 G 是 n 阶有限群,a 是 G 中阶为 s 的元,τ_a 是由 a 确定的集合 G 到集合 G 的右乘变换,即 $\tau_a: G\to G,\quad g\longmapsto ga$. 证明:集合 G 上的置换 τ_a 是 $\dfrac{n}{s}$ 个不相交的 s-轮换的乘积.

18. 设 G 是有限群,且 $|G| = 2^t m$,其中 $t>0$ 且 m 为奇数. 如果 G 中存在 2^t 阶循环子群,证明: G 中存在子群 K,使得 $[G:K] = 2$.

第三章　环、域与模

本章主要介绍有关环、域与模的一些基本概念：它们的子系统、商系统、同态等等. 介绍环、域的一些具体例子：数环、多项式环、矩阵环、数域、有限域等，以及构造环、域的一些基本方法. 作为整数环 $\mathbb{Z}$ 和数域 F 上一元多项式环 $F[x]$ 的整除理论的推广，本章将讨论交换环的整除理论. 在学习后者时，请读者特别注意推广的过程，熟悉和学会从特殊例子到一般情形的推广方法.

§1　环与域

我们已经见到过许多具体环和具体域，诸如数环、数域、多项式环等. 现在我们给出抽象环和抽象域的定义.

定义 1.1　设 R 是一个非空集合，其上有两个二元运算：$+$（加法）和 $\cdot$（乘法），如果这些运算满足下面条件：

R1) $(R, +)$ 是一个交换加群（Abel 群），其恒等元记作 O（称为零元）；

R2) $(R, \cdot)$ 是一个半群；

R3) 乘法对加法的分配律成立：

对任意 $a, b, c \in R$，有

$$a \cdot (b + c) = a \cdot b + a \cdot c,$$
$$(b + c) \cdot a = b \cdot a + c \cdot a.$$

我们就称 $(R, +, \cdot)$ 是一个环. 如果环 R 满足

R4) $(R, \cdot)$ 是一个具有恒等元的半群（称为幺半群），其恒等元记作 e（称为单位元），就称 R 是一个有单位元 e 的环.

如果环 R 满足

R5) 乘法交换律：对任意 $a, b \in R$，有 $a \cdot b = b \cdot a$. 则称 R 为一个交换环.

定义 1.2　设 F 是一个有 e 的交换环. 如果对 F 中任意非零元 a，关于乘法有逆元，即存在 $a^{-1} \in F$ 使 $aa^{-1} = e$，则称 F 为一个域.

先看几个我们已熟悉的例子.

例 1　设 $R = \left\{\dfrac{m}{2^n}, m, n \in \mathbb{Z}\right\}$，则 R 关于数的加法和乘法作成一个有单位元 1 的交换环.

例 2　$\mathbb{C}[x]$ 表示复系数一元多项式的全体，则 $\mathbb{C}[x]$ 关于多项式的加法和乘法作成一个有单位元 1 的交换环.

例 3　令 $C[0,1]$ 表示定义在区间 $[0,1]$ 上的所有连续实函数的集合. 对 $f,g \in C[0,1]$ 规定

函数的加法：对任意 $x \in [0,1]$，$(f+g)(x) = f(x)+g(x)$；

函数的乘法：对任意 $x \in [0,1]$，$(fg)(x) = f(x)g(x)$.

则 $C[0,1]$ 作成一个有单位元 $E(E(x) \equiv 1)$ 的交换环，其零元为 O（$O(x) \equiv 0$）.

例 4　今把上例中函数的定义域和值域推广一下，取任意集 M 来代替 $[0,1]$，并取一个一般的，具有单位元 1 的环 R 来代替实数域，而来考察所有定义在集 M 上，在环 R 中取值的函数 f 的集合 $R\{M\}$. 仍用函数的加法和函数的乘法运算，即若 $f,g \in R\{M\}$，规定

函数的加法：对任意 $x \in M$，$(f+g)(x) = f(x)+g(x)$；

函数的乘法：对任意 $x \in M$，$(fg)(x) = f(x)g(x)$.

关于这些运算，$R\{M\}$ 作成一个有单位元 E（$E(x) \equiv 1$）的环. 验证工作和例 3 是完全一样的. 当 R 是交换环时，$R\{M\}$ 还是交换环. 我们简称 $R\{M\}$ 为函数环.

如果作一个类比的话，可以说交换函数环在交换环类中的作用，有点像变换群（包括线性变换群）在群论中的作用，一旦把一个群解释成变换群，对这个群就可以从几何角度去观察它. 同样，一旦把一个抽象的交换环解释成函数环，则对此函数交换环我们就可以从几何角度（函数的图象）和函数论的角度去观察它，而这是很有意义的事.

例 5　设 $M_n(R)$ 表示含 1 的数环 R 上的 $n \times n$ 矩阵的全体，则 $M_n(R)$ 关于矩阵的加法和乘法作成一个有单元 I（单位矩阵）的非交换环.

在数环中我们有诸如 $0 \cdot a = a \cdot 0 = 0$，$(-a)(-b) = ab$，$(-a) \cdot b = -ab$ 等关系. 这在一般环中是否也成立呢？

先把符号的意义明确一下，设 R 是一个环，则 $(R,+)$ 是交换加群，$(R,\cdot)$ 是乘法半群. 我们规定

$$na = \begin{cases} \underbrace{a + \cdots + a}_{n\text{个}}, & n \text{ 是正整数；} \\ O, & n = 0; \\ \underbrace{(-a) + \cdots + (-a)}_{n\text{个}}, & n \text{ 是负整数，} \end{cases}$$

其中 $-a$ 是 a 关于加法的逆元(负元),即 $a+(-a)=(-a)+a=O$. 其实这就是乘群中元素 a 的幂 a^n 在加群的表示方式.还规定

$$a^n = \underbrace{a\cdot a\cdot\cdots\cdot a}_{n个}, \qquad n \text{ 是正整数}.$$

和我们在群论中讨论的一样,可证得:

$$(m+n)a = ma + na, \quad 对任意\ m,n\in\mathbb{Z}, a\in R,$$

$$a^n\cdot a^m = a^{n+m}, \quad (a^n)^m = a^{nm}, \quad 对任意正整数\ n,m,$$

乘群中 $(ab)^{-1}=b^{-1}a^{-1}$, a^{-1} 的逆元是 a. 在交换加群 $(R,+)$ 中就成为 $-(a+b)=-a-b$, $-(-a)=a$, 一般还有

对任意 $n,m\in\mathbb{Z}, a\in R$, $n(a+b)=na+nb$, $m(na)=(mn)a$. 若环 R 有单位元 e, 由于 $e^2=e$, 我们利用分配律可得:

$$ne + me = (n+m)e, \quad ne\cdot me = (nm)e,$$

$$ne\cdot a = \underbrace{(e+\cdots+e)}_{n个}\cdot a = \underbrace{ea+\cdots+ea}_{n个} = \underbrace{a+\cdots+a}_{n个} = na.$$

命题 1.3 在环 R 中有:

1) $O\cdot a = a\cdot O = O$;

2) $(-a)b = -ab = a(-b)$;

3) $(-a)(-b) = ab$;

4) 若 R 有单位元 e, 则单位元是唯一的.

证明的方法和在数环中的情况一样.只是这里我们每一步推理,都是严格地根据环的定义去作,每一个符号准确地按照环的定义去理解,而不能加入任何环的定义以外的"杂念".例如元素 O,它就是对 $\forall\ a\in R$ 有等式 $a+O=O+a=a$ 的那个元素 O,而 $-ab$ 就是和元素 ab 有等式关系 $ab+(-ab)=(-ab)+ab=O$ 的那个元素 $-ab$. 看看定义中是怎么说的,我们就不会出错,而许多基本事实是很容易证的.

命题 1.3 的证明 1) $O+O\cdot a = O\cdot a = (O+O)\cdot a = O\cdot a + O\cdot a$. 因加群 $(R,+)$ 中有消去律,消去等式两边的 $O\cdot a$ 便得 $O\cdot a = O$. 同理可证 $a\cdot O = O$.

2) 欲证 $(-a)b=-ab$, 只需证明 $(-a)b+ab=O$, 因为这将意味着 $(-a)b$ 和 $-ab$ 都是同一元素 ab 的负元,它们当然就相等了.由

$$(-a)b + ab = ((-a)+a)b = O\cdot b = O,$$

故得.

3) 和 2)类似,只需证明 $(-a)(-b)+(-ab)=O$ 即可.由

$$(-a)(-b)+(-ab)=(-a)(-b)+(-a)b=(-a)((-b)+b)$$
$$=(-a)\cdot O=O,$$

故得.

4) 这等于要证明乘法半群 $(R,\cdot)$ 的恒等元是唯一的.这和群的恒等元是唯一的证明是一样的.留给读者.□

这里我们简化一下符号.把环 R 中的零元 O 用 0 来表示,把环 R 中唯一的单位元 e 用 1 来表示, $ne, n\in\mathbb{Z}$ 就用 n 来表示.

上面我们看到的,无论是 ne, me 彼此之间的加法、乘法运算,也无论是 ne 和环 R 中其它元素 a 的乘法运算: $ne\cdot a=na=a\cdot ne$,都说明这些元素 $ne, n\in\mathbb{Z}$ 在环 R 中运算的地位和普通整数 n 在数环中的地位是一样的.这就使得这种简化符号,即把 ne 和 n 等同起来,既合法又方便.我们将这样而把全体整数直接看成有单位元 1 的环中的元素.这里唯一要注意的是,作为通常整数,3 当然不等于 6,但在某个环 R 中完全可能 $3e=6e$,因而在该环 R 中, $3=6$.当你把整数 n 看成环 R 中元素感到有些没把握时,那你就把 n 换成 ne 去考虑,不清楚的地方就迎刃而解了.

现在定义子环,商环和环的同态.

这里你可用两种办法与我们熟悉的事物对比.一种是和集合类比,而把环看作是具有两个运算的集合,当我们讨论群时,曾作过这样的类比.另一种是和群类比,把环看作是具有一个乘法运算的交换加群,即设想加群是基础而乘法是环的"灵魂".

定义 1.4 R 是一个环, A 是 R 的一个非空子集.如果 A 满足下列条件:

1) A 是 $(R,+)$ 的子群;

2) A 关于乘法封闭,

就称 A 是 R 的一个子环.

子环 A 本身是一个环,因为 $(A,+)$ 是加群, $(A,\cdot)$ 是乘法半群,在 A 中也有乘法对加法的分配律,这是因为分配律在 R 中成立,因而对属于 A 的元素当然也成立.

易见 $A=\{0\}$ 是子环.这个由一个元素组成的环称为零环.只有在零环中加群的零元 0 和关于乘法的单位元 1 是重合的.

R 本身当然也是环 R 的一个子环,不同于 $\{0\}$ 和 R 的子环称为 R 的非平

凡子环.和一些子群之交仍是子群一样,我们有

命题 1.5 R 是环,而 Σ 是 R 的一些子环组成的非空集合. $\bigcap_{A\in\Sigma}A$ 是一个子环.□

和群论类似,我们可以如下定义由环 R 的子集 S 生成的子环 $\langle S\rangle$.

定义 1.6 R 是环, S 是 R 的非空子集. R 中含 S 的最小子环,称为 S 在 R 中生成的子环.记作 $\langle S\rangle$, 并称 S 为 $\langle S\rangle$ 的生成元集.

令 Σ 是由 R 中一切含 S 的子环组成的集合.因为 $R\in\Sigma$, 故 Σ 不空.显然 $\bigcap_{A\in\Sigma}A$ 为 R 中含 S 最小的子环.即 $\langle S\rangle=\bigcap_{A\in\Sigma}A$.

若 R 是有 1 的环,则 $\langle 1\rangle=\{n,n\in\mathbb{Z}\}$. 这是因为,设 $\overline{\mathbb{Z}}=\{n,n\in\mathbb{Z}\}$, 一方面 $(\overline{\mathbb{Z}},+)$ 是 $(R,+)$ 的子群, $\overline{\mathbb{Z}}$ 关于乘法是封闭的,因而 $\overline{\mathbb{Z}}$ 是环 R 的子环;另一方面,如果 A 是 R 的子环且 $1\in A$, 则 $1+1=2\in A$, 一般"正整数" $n\in A$, 又 $-1\in A$, 随之"负整数" $m\in A$. 当然 0(环的零元)永远在任一子环中,故 $\overline{\mathbb{Z}}\subseteq A$, 即 $\overline{\mathbb{Z}}$ 是含 1 的最小子环.

例 6 令 $A=A[0,1]$ 表示定义在 $[0,1]$ 上的所有无限次可微分的实 n 元 $(x_1,\cdots,x_n)$ 函数的集合.定义 $\mathbb{R}$ 到 A 的数乘运算 αf 为 $(\alpha f)(x_1,\cdots,x_n)=\alpha(f(x_1,\cdots,x_n))$, 这里 $\alpha\in\mathbb{R}$, $f\in A$. 则 A 关于函数的加法以及 $\mathbb{R}$ 到 A 的数乘运算作成一个实数域 $\mathbb{R}$ 上的无限维向量空间.

令 T 表 $\mathbb{R}$-空间 A 的所有线性变换的全体,两个线性变换 t,s 的加法、乘法定义为

$$(t+s)(g)=t(g)+s(g),$$
$$(ts)(g)=t(s(g)),$$

则 $(T,+,\cdot)$ 作成一个有 1 的环.请读者注意一下变换的加法和函数的加法是一样的,但线性变换的乘法和函数的乘法是完全不一样的.取 S 为 n 个偏微分算子 $\frac{\partial}{\partial x_i}$, $i=1,2,\cdots,n$ 的集合,依定义 $\frac{\partial}{\partial x_i}(f)=\frac{\partial f}{\partial x_i}$, 直接验证知 $\frac{\partial}{\partial x_i}$ 是 $\mathbb{R}$-空间 A 的线性变换,因而 $S\subseteq T$, 称 $R=\langle\mathbb{R}\cup S\rangle$ 为 $\mathbb{R}$-空间 A 上的微分算子环;它是一个有 1 的变换环;如果把偏微分算子 $\frac{\partial}{\partial x_i}$ 的乘积 $\underbrace{\frac{\partial}{\partial x_i}\cdot\frac{\partial}{\partial x_j}\cdot\cdots\cdot\frac{\partial}{\partial x_k}}_{n个}$ 简记作 $\frac{\partial^n}{\partial x_i\partial x_j\cdots\partial x_k}$, 则 R 中元素都可写成

$$\sum\alpha_{i,j,\cdots,k}\frac{\partial^n}{\partial x_i\partial x_j\cdots\partial x_k},\ \alpha_{i,j,\cdots,k}\in\mathbb{R}$$

的形状.

现在来讨论两个环之间的关系.

我们已经知道两个集合之间的关系就是指它们之间的那些映射,而两个群的关系就是指它们的同态映射.这里读者该也会想到应如何去定义环 R 到环 R' 的同态对应.

定义 1.7　R,R' 是两个环,ϕ 是集 R 到集 R' 的一个映射,如果

1) ϕ 是加群 $(R,+)$ 到 $(R',+)$ 的同态映射,即对任意 $x,y\in R$,$\phi(x+y)=\phi(x)+\phi(y)$.

2) ϕ 保持乘法,即有 $\forall\ x,y\in R$,$\phi(xy)=\phi(x)\phi(y)$.

则称 ϕ 为环 R 到环 R' 的的同态映射.用 $\mathrm{Im}\phi=\{\phi(x),x\in R\}$ 表示 ϕ 的象,用 $\mathrm{Ker}\phi=\{x\in R\mid\phi(x)=0\}$ 表示 ϕ 的核.

与群的同态类似,可定义环的单同态、满同态、同构等概念.

例 7　设 $\mathbb{Z}$ 是整数环,而 R 是有 1 的环,规定映射

$$\begin{aligned}\phi:\mathbb{Z}&\longrightarrow R\\ n&\longmapsto n\in\langle 1\rangle.\end{aligned}$$

我们上面的讨论说明 ϕ 是保持加法,保持乘法的.因而 ϕ 是整数环 $\mathbb{Z}$ 到环 R 的一个同态,也是整数环 $\mathbb{Z}$ 到环 $\langle 1\rangle$ 上的一个满同态,但一般不是同构.

例 8　设 $C[0,1]$ 是 $[0,1]$ 上的连续实函数环.取点 $p\in[0,1]$ 而规定

$$\begin{aligned}\phi:C[0,1]&\longrightarrow\mathbb{R}\\ f(x)&\longmapsto f(p).\end{aligned}$$

直接验证知 ϕ 是环 $C[0,1]$ 到 $\mathbb{R}$ 的一个同态,易知 ϕ 还是一个满同态,即 $\mathrm{Im}\phi=\mathbb{R}$.　$f(x)$ 对应到 $0\in\mathbb{R}$ 当且仅当 $f(x)$ 在 p 点上的值是 0,即 $\mathrm{Ker}\phi=\{f(x)\in C[0,1]\mid f(p)=0\}$. 还易见,$f(x),g(x)$ 在 ϕ 下有相同的象当且仅当 $f(p)=g(p)$. 读者若画出 $f(x)$ 的图象,就可更具体地看到这个同态 ϕ 的内容.

在群论中我们已经看到,群 G 的合同、商群、正规子群以及群 G 到其它群上的满同态基本上是一回事,是一个事物的不同面孔.例如,群 G 的合同决定一个商群和群到其商群的满同态,而同态的核又是 G 的正规子群.在环论中,环 R 的合同、商环、理想以及环 R 到其它环上的满同态也基本是一回事.在群论中我们是从合同开始的,这次我们从同态出发,结果是一样的.

设 ϕ 是环 R 到环 R' 的一个同态,而令 $I=\mathrm{Ker}\phi=\{x\in R\mid\phi(x)=0\}$

$\subseteq R$. 易见 R 的子集 I 是子环,这是因为,若 $a,b \in I$, 则有 $\phi(a)=\phi(b)=0$, 由

$$\phi(a+b)=\phi(a)+\phi(b)=0+0,$$
$$\phi(ab)=\phi(a)\phi(b)=0\cdot 0=0$$

知 $a+b, ab \in I$. 从最后一个式子还可看出,当 a,b 中只有一个属于 I, 那么 ab 就在 I 中.就是说,若 $a\in I, r\in R$, 则有

$$\phi(ra)=\phi(r)\phi(a)=\phi(r)\cdot 0=0,$$
$$\phi(ar)=\phi(a)\phi(r)=0\cdot\phi(r)=0,$$

因而 $ar, ra \in I$. 这表明 $I=\mathrm{Ker}\phi$ 这个子集比子环的性质还要更好一些.

定义 1.8 若环 R 的非空子集 I 满足下面条件:

1) I 是一个子加群;

2) 对任意 $a\in I, r\in R$, 元素 ar, ra 都在 I 中.

此时我们称 I 是环 R 的一个理想.

和在群论中一样,在环 R 的子集 A,B 间也引入加法和乘法如下:规定

$$A+B=\{a+b \mid a\in A, b\in B\},$$

$$AB=\left\{\sum_{i=1}^{n} a_i b_i \mid n\in\mathbb{N}, a_i\in A, b_i\in B, 1\leqslant i\leqslant n\right\},$$

由于加法交换故有 $A+B=B+A$.

命题 1.9 设 I 是环 R 的理想,则 I^2 是环 R 的理想,更一般 $I^n=I^{n-1}\cdot I$ 也是 R 的理想.□

设 I 是环 R 的理想.由于 $(R,+)$ 是交换加群,故 $(I,+)$ 是 $(R,+)$ 的正规子群.作商加群 $R/I=\{a+I \mid a\in R\}$. 今在此加群 R/I 上再引进一个乘法而规定

$$\forall\ a,b\in R, (a+I)\cdot(b+I)=ab+I. \tag{1}$$

首先要解决的是这个规定是合理的,即要解决:若 $a+I=a'+I, b+I=b'+I$, 则也有 $ab+I=a'b'+I$. 我们知道: $x+I=y+I$ 当且仅当 $x-y\in I$, 或当且仅当 $x=y+i, i\in I$. 这样我们该证 $a'b'-ab\in I$. 注意到 $a'=a+i, b'=b+j, i,j\in I$, 故有

$$a'b'-ab=(a+i)(b+j)-ab=aj+ib+ij\in I,$$

这样(1)给出 R/I 的一个乘法.

今证 $(R/I,+,\cdot)$ 作成一个环.为此只需验证一下乘法对加法的分配律成立,这由

$$\begin{aligned}(a+I)((b+I)+(c+I))&=(a+I)((b+c)+I)=a(b+c)+I\\&=(ab+ac)+I=(ab+I)+(ac+I)\\&=(a+I)(b+I)+(a+I)(c+I),\end{aligned}$$

以及类似地对从右侧去乘的计算,便得.

定义 1.10　我们称环 $(R/I, +, \cdot)$ 为环 R 关于理想 I 的商环,其中 $R/I = \{a+I, a\in R\}$,

$$(a+I)+(b+I)=(a+b)+I,\quad (a+I)\cdot(b+I)=ab+I.$$

定理 1.11　R 是环,而 R/I 是 R 关于理想 I 的商环.令

$$\begin{aligned}\phi: R &\longrightarrow R/I\\ a &\longmapsto a+I,\end{aligned}$$

则 ϕ 是环 R 到 R/I 上的同态,称之为环 R 到其商环 R/I 上的自然同态.

证明　在没有混淆的时候.我们常把 $a+I$ 简记作 $[a]$.设 $a,b\in R$,则有

$$\phi(a+b)=[a+b]=[a]+[b]=\phi(a)+\phi(b),$$
$$\phi(ab)=[ab]=[a][b]=\phi(a)\phi(b),$$

故得.□

同环 R 的子集 S 生成子环 $\langle S\rangle$ 一样,我们可以定义 S 在环 R 中生成的理想就是环 R 中包含 S 的最小理想,把它记成 (S).并称 (S) 为由 S 生成的理想,称 S 为 (S) 的生成元集.(S) 是存在的,因为一些理想之交仍是理想(证明!),故 R 中含 S 的所有理想(R 就是其中一个)之交就是 (S).另一方面从 S 出发我们可把 (S) 的元素具体写出来,这就是当环 R 有 1 时,

$$(S)=\sum_{s\in S}sR+\sum_{s\in S}Rs+\sum_{s\in R}RsR\quad(\text{有限和}),\tag{1}$$

而当 R 是有 1 的交换环时,

$$(S)=\sum_{s}sR\quad(\text{有限和}).\tag{2}$$

等式(1)之所以成立,是因为(1)之右侧元素都应在 (S) 中,而(1)的右侧已经是一个包含 S 的理想(证明!),因而包含 (S),合在一起便得(1).当乘法交换时,(1)就变成(2).

下面给出几个商环的例子,特别是前两个是以后常用到的.

例 9　$\mathbb{Z}$ 是整数环,$(n)=\{$整数 n 的所有倍数$\}$.它是 $\mathbb{Z}$ 的理想,商环 $\mathbb{Z}/(n)$ 是一个有单位元的交换环.令 $[t]=t+(n)$.则 $[t]=[s]$ 当且仅当 $t-s\in(n)$,当且仅当 $n\mid(t-s)$,当且仅当 t,s 被 n 除时有相同的余数.因而 $\mathbb{Z}/(n)$ 只有 n 个元素,这就是

$$\begin{aligned}[0]&=\{mn, m\in\mathbb{Z}\},\\ [1]&=\{mn+1, m\in\mathbb{Z}\},\\ &\cdots\cdots\\ [n-1]&=\{mn+(n-1), m\in\mathbb{Z}\},\end{aligned}$$

这是我们看到的第一个有限环,即元素个数为有限的环.

当 p 是素数时, $\mathbb{Z}/(p)$ 还是一个有限域,即元素为有限的域. 注意到 $[t] = [0]$ 当且仅当 $p|t$, 当 $[t] \neq [0]$, 即 $p \nmid t$, 随之 p, t 互素. 由整数论可知存在整数 m, n, 使得 $np + tm = 1$, 随之在 $\mathbb{Z}/(p)$ 中有

$$[1] = [np + mt] = [tm] = [t][m],$$

即得 $[m]$ 是 $[t]$ 的乘法逆元,这就证明了 $\mathbb{Z}/(p)$ 是一个域.

当 $p = 2$ 时, $\mathbb{Z}/(2)$ 有下面的运算表(表中把 $[0],[1]$ 简记作 0,1)

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

当 $p = 3$ 时, $\mathbb{Z}/(3)$ 有下面的运算表(表中把 $[0],[1],[2]$ 记作 0,1,2)

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

通常将把环 $\mathbb{Z}/(n)$ 简记作 $\mathbb{Z}_n$. 在群论中我们见到过它,那时它只是一个加群. 而当 p 是素数时, $\mathbb{Z}_p$ 还是域. 这些有限域 $\mathbb{Z}_p$ 是很有用处的,例如在编码、有限几何、实验设计等课题中. 应该把它们和有理数域同样看待.

例 10 设 $F[x]$ 是数域 F 上一元多项式环. 任取定一 n 次多项式 $f(x)$ 而考察商环 $R = F[x]/(f(x))$, 这里 $f(x)$ 生成的理想 $(f(x)) = \{f(x) \cdot g(x), \forall\ g(x) \in F[x]\}$. 令 $[g(x)] = g(x) + (f(x))$.

设 $g(x)$ 被 $f(x)$ 除时的余式为 $r(x)$, 则有 $[g(x)] = [r(x)]$. 这时 R 中的任何元素都可写成 $[g(x)]$, 其中 $g(x) = 0$ 或 $g(x)$ 的次数 $< n$, 且在此约定下 $[g(x)] = 0$ 当且仅当 $g(x) = 0$.

和 $\mathbb{Z}/(p)$ 的情况完全一样, 当 $f(x) = p(x)$ 是不可约多项式时, $F[x]/(p(x))$ 也是一个域. 为此只需证明它的非 0 元素 $[g(x)] \neq [0]$ 有逆元. 由 $[g(x)] \neq [0]$ 知 $p(x) \nmid g(x)$, 但 $p(x)$ 是不可约的, 故 $p(x)$ 和 $g(x)$ 互素, 这时知必有多项式 $s(x)$ 和 $t(x)$ 使得 $s(x)p(x) + t(x)g(x) = 1$, 随之在 $F[x]/(p(x))$ 中有

$$[1] = [s(x)p(x) + t(x)g(x)] = [t(x)g(x)] = [t(x)][g(x)],$$

即 $[g(x)]$ 有逆元 $[t(x)]$.

和群论中的第一同态定理一样,这里也有

定理 1.12 (环的第一同态定理) 设 ϕ 是环 R 到环 R' 的满同态，$I=\mathrm{Ker}\phi$，则商环 $R/I\cong R'$.

证明 作映射

$$\begin{aligned}\psi: R/I &\longrightarrow R'\\ a+I &\longmapsto \phi(a).\end{aligned}\tag{4}$$

首先要说明 ψ 的定义是合理的，即需证 $a+I$ 的象 $\phi(a)$ 与代表 a 的选择无关，也就是要证：若 $a+I=b+I$，则必有 $\phi(a)=\phi(b)$. 由 $a+I=b+I$ 得 $a=b+i, i\in I$，于是有

$$\phi(a)=\phi(b+i)=\phi(b)+\phi(i)=\phi(b)+0=\phi(b).$$

在证明了上面的规定(4)确定义了一个映射 ψ 之后，验证 ψ 保持运算就是很容易的事了. 我们把它留给读者. □

这里定理说明 R 的商环穷尽了 R 的满同态象：商环是满同态象，满同态象就是商环. 这样一个环 R 和其它环的关系在一定意义下归结为 R 与其商环的关系，即环 R 与外部世界的关系归结为环 R 自身的内部结构.

这样，对环我们也完成了对商环、理想、同态的介绍. 我们这里没有明确提出环的合同概念. 然而相信读者一定自己能给出环的合同关系的定义，或者从上面的讨论，或者模仿群论中的相应讨论而自己去证明：环 R 的合同关系 $\sim$ 都是由环 R 的一个理想 I 按下列方式定义的：$a\sim b$ 当且仅当 $a-b\in I$. 当然不去讨论环的合同关系也是完全可以的：对于环论而言知道理想 I，商环 R/I 以及第一同态定理也就够了.

但这里还是给出下面半群的例子. 一切正整数作成的集合 $\mathbb{Z}^+$ 关于数的乘法是一个半群. 集 $\mathbb{Z}^+$ 的等价关系(划分)：$\{1\},\{2,3,4,\cdots\}$ 或 $\{1,2\},\{3,4,\cdots\}$ 显然与乘法是和谐的，因而是半群 $\mathbb{Z}^+$ 的合同划分. 我们看到它们是很没有规则. 事实上除了以群为基础的代数系统(如环和以后的模)外，一般代数系统的合同关系可能是很难掌握的.

应该再提一下的是：商环 R/I 的元素是加群 R 中子加群 I 的陪集，我们在子加群 I 上加了一些乘法条件就是为了使得这个关于加法的合同关系也是与乘法和谐的，就是说，在作商环时，环的加法是基础. 因而我们可以设想，关于群的一些同态定理，只要把群换成环，把正规子群换成理想，完全保留原来的形式，对环也是成立的.

下面把环的第二同态定理写出，仍略去证明.

定理 1.13(环的第二同态定理) 设 ϕ 是环 R 到环 $\overline{R}$ 上的满同态，$I=\mathrm{Ker}\phi$，令

$$L(R,I)=\{R \text{ 中所有包含 } I \text{ 的子环}\},$$
$$L(\overline{R})=\{\overline{R} \text{ 中所有子环}\},$$

则

$$\begin{aligned}\theta: L(R,I) &\longrightarrow L(\overline{R})\\ S &\longmapsto \phi(S)=\{\phi(s),s\in S\}=\overline{S}\end{aligned}$$

是集 $L(R,I)$ 到集 $L(\overline{R})$ 上的一个一一对应,且有

1) $S\supseteq T$ 当且仅当 $\overline{S}\supseteq\overline{T}$;

2) S 是 R 的理想当且仅当 $\phi(S)$ 是 $\overline{R}$ 的理想;

3) 当 S 是 R 的理想时,有 $R/S\cong\overline{R}/\overline{S}$.

练习

1. 设 R 是一个环,

1) 求证: $C(R)=\{c\in R \mid \text{对任意的 } x\in R \text{ 有 } cx=xc\}$ 是 R 的子环,称 $C(R)$ 为 R 的中心;

2) 求证: R 是除环,则 $C(R)$ 是域.

2. 设 I 是环 R 的一个理想,求证: $A=\{r\in R \mid \text{对任意的 } x\in R, \text{有 } xr\in I\}$ 是 R 的理想,并包含 I.

3. 设 R 是环, I 是 R 的理想, H 是 R 的子环,证明:

1) $H+I$ 是 R 的子环, I 是 $H+I$ 的理想, $H\cap I$ 是 H 的理想;

2) $H+I/I\cong H/H\cap I$.

4. 设 I,J 是环 R 的理想,且 $I\subseteq J$,求证:

$$(R/I)/(J/I)\cong R/J.$$

5. 设 $\phi: R\to\overline{R}$ 为环同态,求证:

1) R 是域,则 $\mathrm{Ker}\phi=0$ 或 $\mathrm{Ker}\phi=R$;

2) R 是域,且 ϕ 是环同构,则 $\overline{R}$ 也是域.

6. 设 m,r 是正整数,且 $r\mid m$. 令 $\phi:\mathbb{Z}_m\to\mathbb{Z}_r, \bar{a}\longmapsto\bar{a}$,求证: ϕ 是 $\mathbb{Z}_m$ 到 $\mathbb{Z}_r$ 的环同态,并求 $\mathrm{Ker}\phi$, $\mathbb{Z}_m/\mathrm{Ker}\phi$.

§2 环的构造

我们知道数环、多项式环、函数环、微分算子环、线性变换环以及更一般的算子环,这些具体环是一般环论的支柱,没有它们也就没有环论了. 另一方面,我们常需要知道更多的环,从已知环构造新环,或者就是硬构造出新环来,就像我们过去构造自由群那样. 上面已经看到利用子环和商环的概念可从已知环构造新环,特别如 $\mathbb{Z}_n=\mathbb{Z}/(n)$, $F[x]/(f(x))$ 等等.

有时为了某种方便或需要,我们希望将已知的环扩展成新的环. 数的扩展

是一个最好的样板，它提供了丰富的内容和启发. 从运算的角度来看，当人们只知道自然数时，加法是可通行的，但减法不行，于是人们希望扩大数的概念使减法也能够施行，这就有了 $\mathbb{Z}$. 在 $\mathbb{Z}$ 中乘法没问题，但除法不行，于是要构造 $\mathbb{Q}$· $\mathbb{Q}$ 中求极限不完美，为了求极限能顺利执行，于是构造实数域 $\mathbb{R}$. 甚至 x^2+1 在 $\mathbb{R}$ 中也无解，于是希望扩大数的概念使得每一多项式在其中都能有根. 这当然不是历史上数的逐步扩大的过程和原因，例如历史上是由自然数先扩到正有理数，然后才是负数，而承认虚数的存在和引入它，首先由于求实三次方程的实根的计算公式中出现了虚数而又无法避免. 然而今日如上述那样看数的扩张也还是自然的，特别是启发我们作出下面的构造.

先引入一类与整数环 $\mathbb{Z}$ 类似的交换环类.

定义 2.1 1) 设 R 是一个环. 若 $a,b\in R, a\neq 0, b\neq 0$ 而 $ab=0$，则称 a 为左零因子，b 为右零因子. 常简称为零因子.

2) 设 R 是一个环，称 R 中有左消去律，如果由 $ab=ac$ 及 $a\neq 0$ 可得 $b=c$.

定义 2.2 称一个有 1 的交换环 R 为整环，如果 R 中没有零因子.

命题 2.3 有 1 的交换环 R 是整环当且仅当在 R 中消去律成立.

证明 这就是要证：在交换环 R 中无零因子和有消去律是等价的. 先设 R 中无零因子，此时由 $ab=ac$，可得 $a(b-c)=0$，如果又知 $a\neq 0$，则由假设知 $b-c=0$，即 $b=c$. 再设 R 中有消去律，若 $ab=0$，而 $a\neq 0$，则由 $ab=a\cdot 0$ 及消去律得 $b=0$，即 R 中不会有零因子. □

易见任意域的有 1 子环都是整环. 今证任意整环必可看作某个域的子环，也就是模仿从 $\mathbb{Z}$ 作 $\mathbb{Q}$ 的方法，把一个非零元素不一定有逆的整环扩大成一个域.

设 R 是一个整环. 令 $F=\{(a,b)\mid a,b\in R, b\neq 0\}$.

这里把 (a,b) 看成一个符号，而我们心中把它想成是“a 除以 b”. 其实也可以写成 a/b，但“/”容易由于和除法的记号相混淆而引起麻烦，因而我们干脆选用符号 (a,b).

由于我们的目的，下面在集 F 中引进的等价关系 $\sim$ 则是自然的也是必须的. 规定：$(a,b)\sim(c,d)$ 当且仅当 $ad=bc$. 我们只来验证它满足等价关系的第三个条件—— 传递律. 设 $(a,b)\sim(c,d)$，$(c,d)\sim(e,f)$，则有

$$ad=bc,\quad cf=de,$$

因而有

$$adf = bcf = bde.$$

注意到 $d \neq 0$ 而交换环 R 是整域，故消去 d 而有 $af = be$，即 $(a,b) \sim (e,f)$. 把在关系 $\sim$ 下，(a,b) 所在的等价类 $[(a,b)]$ 简记作 $[a,b]$. 而令 $\overline{F} = \{[a,b],(a,b) \in F\}$.

还是根据我们的目的，下面在集 $\overline{F}$ 中引进的运算是自然的和必须的. 规定：

$$[a,b] + [c,d] = [ad + bc, bd]; \tag{1}$$

$$[a,b] \cdot [c,d] = [ac, bd]. \tag{2}$$

这里必须证明上面运算的规定与所用代表的选择无关，即是要证若 $(a,b) \sim (a',b')$（即 $[a,b] = [a',b']$），$(c,d) \sim (c',d')$ 则必有

$$(ad + bc, bd) \sim (a'd' + b'c', b'd'), \tag{3}$$

$$(ac, bd) \sim (a'c', b'd'). \tag{4}$$

我们来验证(4)，而把(3)留给读者. 由假设知

$$ab' = a'b, \quad cd' = c'd,$$

因而两式相乘即得

$$ab'cd' = a'bc'd.$$

而此式意味着(2)是与代表的选择无关. 这就证明(1),(2)两式的确定义了 $\overline{F}$ 的两个运算.

今证 $(\overline{F}, +, \cdot)$ 是一个有单位元的交换环. 由(1),(2)可看出，$\overline{F}$ 中元素 $[a,b],[c,d]$ 间的运算完全归结为环 R 中元素 a,b,c,d 之间的运算. 利用整域 R 中运算的性质可推得 $\overline{F}$ 中运算的性质. 例如，一眼从(2)就看出，$\overline{F}$ 中乘法是适合结合律，交换律的，以及 $\overline{F}$ 是没有零因子的. 由

$$[1,1] \cdot [a,b] = [a,b] \cdot [1,1] = [a,b],$$

$$[0,1] + [a,b] = [a,b] + [0,1] = [a,b]$$

知 $[1,1]$ 是 $\overline{F}$ 的单位元，而 $[0,1]$ 是 $\overline{F}$ 的零元. 我们在这里再验证一下 $\overline{F}$ 中的分配律，而把其余的验证工作留给读者. 我们计算

$$\begin{aligned}[a,b]([c,d] + [e,f]) &= [a,b][cf + de, df] \\ = [a(cf + de), bdf] &= [acf, bdf] + [ade, bdf].\end{aligned}$$

但

$$[acf, bdf] = [ac, bd] = [a,b] \cdot [c,d],$$

$$[ade, bdf] = [ae, bf] = [a,b] \cdot [e,f],$$

故得分配律成立.

现已得 $(\overline{F}, +, \cdot)$ 是一个有单位元 $[1,1]$ 的交换环. $\overline{F}$ 还是一个域，因为若 $[a,b] \neq [0,1]$，即 $a \neq 0$，则易见 $[a,b] \cdot [b,a] = [ab, ab] = [1,1]$，即 $[a,b]$ 有逆元 $[b,a]$. 作映射

$$\begin{aligned}\phi: R &\longrightarrow \overline{F}\\ a &\longmapsto [a,1].\end{aligned}$$

易见 ϕ 是环 R 到域 $\overline{F}$ 内的单同态. 如果用 $\bar{a}$ 来代替 $[a,1]$, 则 $\phi(R)=\{\bar{a}, a\in R\}=\overline{R}$ 是 $\overline{F}$ 的一个子环. 再由

$$[a,b]=[a,1]\cdot[1,b]=[a,1]\cdot[b,1]^{-1},$$

便可把 $\overline{F}$ 中的元素 $[a,b]$ 写成 $\bar{a}\bar{b}^{-1}$, 即 $[a,b]=\bar{a}\bar{b}^{-1}$.

总结一下,就是给定环 R 同构于 $\overline{R}=\{\bar{a}=[a,1], a\in R\}\subseteq\overline{F}$, 且域 $\overline{F}=\{\bar{a}\bar{b}^{-1}, \bar{a}, \bar{b}\in\overline{R}\}$. 如果我们再进一步,把彼此一一对应着的 $\bar{a}$ 和 a 再等同起来,便得 $\overline{F}=\{ab^{-1}, a, b\in R\}$. 这也正是我们最初心目中想作的那个域.

定义 2.4　称如上作出的域 $\overline{F}=\{ab^{-1}, a, b\in R\}$ 为整环 R 的分式域.

易见整数环 $\mathbb{Z}$ 的分式域为 $\mathbb{Q}$. 数环 $R=\{\frac{n}{2^m}\}, n, m\in\mathbb{Z}\}$ 的分式域也是 $\mathbb{Q}$,而 $\mathbb{Q}$ 的分式域则仍是 $\mathbb{Q}$. 下面还会看到其他例子.

这样,任意整环都可扩大成一个除法可行的域. 整环不是孤立存在的而永远可以把它看成一个域的子环,这在某些时候是有好处的,方便的.

这个构造分式域的方式还可以推广,例如 R 没有单位元也行,又例如不去构造域,只是构造一个含 R 的环,使在其中 R 的部分元素有逆,等等.

下面我们模仿利用 Cauchy 序列从有理数构造实数的方法来从一个给定环 R 来构造新的环.

先用对我们方便的形式回忆一下数学分析中 Cauchy 序列的定义. 若 $\{a_n\}$ 是一个有理数序列,称之为 Cauchy 序列,如果任给 $\varepsilon>0$, $\exists N$ 使得对任意 $m>n>N$ 都有 $|a_m-a_n|<\varepsilon$. 这等价于说:取定一组包含 0 的开区间套,例如 $I_n=(-\frac{1}{2^n},\frac{1}{2^n}), n\in\mathbb{Z}^+$, 对任意指定开区间 I_t, 必存在 N 使得 $m>N, n>N$ 时有 $a_m-a_n\in I_t$.

对任意(交换或不交换)环 R, 设 I 是 R 的理想且有性质 $\forall\ n, I^n\supset I^{n+1}$ 及 $\bigcap_{n=1}^{\infty} I^n=\{0\}$. 今把 I^n 类比于开区间 I_n, 而把 $I\supseteq I^2\supseteq\cdots\supseteq I^n\supseteq\cdots$ 看成是环 R 的包含 0 的一个"区间套",这样就可如下把 Cauchy 序列的概念搬到环 R 中来:设 $\{a_n\}, a_n\in R$, 是环 R 中的一个序列,如果对任意指定的 I^t, 必存在 N 使得当 $m>N, n>N$ 时有 $a_m-a_n\in I^t$, 我们就称它为环 R 的一个(I - 进)Cauchy 序列. 有了 Cauchy 序列概念之后,就像过去通过关于极限的完备化从有理数域构造实数一样,下一步该把 Cauchy 序列当作元素(我们心目中该 Cauchy 序列应有的那个极限)看,自然地引入 Cauchy 序列的相等概

念，Cauchy 序列间的加法、乘法等概念.

令 $C=\{$环 R 中所有的 Cauchy 序列$\}$. 规定集 C 的一个等价关系 $\sim$: $\{a_n\}\sim\{b_n\}$ 当且仅当对任意指定的 I^t，必存在 N，当 $m>N$ 时有 $a_m-b_m\in I^t$. 容易验证，$\sim$ 确是一个等价关系，而把 $\{a_n\}$ 所在的等价类记作 $[\{a_n\}]$.

令 $\overline{C}=\{[\{a_n\}],\{a_n\}\in C\}$. 规定集 $\overline{C}$ 的加法和乘法如下：

$$[\{a_n\}]+[\{b_n\}]=[\{a_n+b_n\}], \tag{5}$$

$$[\{a_n\}]\cdot[\{b_n\}]=[\{a_nb_n\}]. \tag{6}$$

现在来证明(5)，(6)的确给出集 $\overline{C}$ 的两个运算. 为此，首先要证明：若 $\{a_n\}$，$\{b_n\}$ 是 Cauchy 序列，则 $\{a_n+b_n\}$，$\{a_nb_n\}$ 也是 Cauchy 序列. 易知对任意指定的 I^t，必存在 N 使 $m>N, n>N$ 时不但 $a_m-a_n\in I^t$ 并且 $b_m-b_n\in I^t$，这时，注意到 I^t 是理想，也有

$$(a_m+b_m)-(a_n+b_n)=(a_m-a_n)+(b_m-b_n)\in I^t,$$

$$a_mb_m-a_nb_n=(a_m-a_n)b_m+a_n(b_m-b_n)\in I^t.$$

这就证明了 $\{a_n+b_n\}$，$\{a_nb_n\}$ 也是 Cauchy 序列. 其次要证明(5)，(6)的规定，与代表的选择无关，例如来证(6)与代表的选择无关，即要证若 $\{a_n\}\sim\{a'_n\}$，$\{b_n\}\sim\{b'_n\}$，则必有 $\{a_nb_n\}\sim\{a'_nb'_n\}$. 由假设知，对任意指定的 I^t，必存在 N 使 $m>N$ 时 $a_m-a'_m\in I^t, b_m-b'_m\in I^t$，这时便也有

$$a_mb_m-a'_mb'_m=(a_m-a'_m)b_m+a'_m(b_m-b'_m)\in I^t,$$

即 $\{a_nb_n\}\sim\{a'_nb'_n\}$. 总起来便证明了(5)(6)确给出 $\overline{C}$ 的运算.

直接验证可知 $(\overline{C},+,\cdot)$ 是一个环，它的单位元是 $[\{1\}]$，而零元是 $[\{0\}]$，其中 $\{a\}$ 表示序列：$a,a,\cdots,a,\cdots$，它显然是一个 Cauchy 序列. 当 R 是交换环时，$\overline{C}$ 也是交换环.

设 $\overline{R}=\{[\{a\}],a\in R\}$. 易见 $\overline{R}$ 是环 $\overline{C}$ 的子环，且映射

$$\begin{aligned}\phi:\ R&\longrightarrow\overline{R}\\ a&\longmapsto[\{a\}]\end{aligned}$$

是 R 到 $\overline{R}$ 上同构对应，也可以说是环 R 到环 $\overline{C}$ 内的同构嵌入.

定义 2.5 设 I 是环 R 的理想且有性质 $\bigcap_{n=1}^{\infty}I^n=\{0\}$. 称如上作出的环 $\overline{C}=\{[\{a_n\}],\{a_n\}$ 是环 R 的 I-进 Cauchy 序列$\}$为环 R 在 I-进拓扑下的完备化，或简称 $\overline{C}$ 为 R 的 I-进完备环.

从上面我们可以看到，一旦把 Cauchy 序列的概念搬到环中而引入 I-进 Cauchy 序列后，剩下来该定义什么，该如何去证，就完全是重复数学分析中我

们熟悉的由有理数域到实数域的构造方法.如果愿意的话,你可以继续模仿下去,而去证 $\overline{C}$ 在 $\overline{I}$ - 进拓扑下的完备化就是 $\overline{C}$ 本身.我们不在这里讨论了.(这里 $\overline{I}$ 是 I, 把它看成是 $\overline{C}$ 的子集,在 $\overline{C}$ 中生成的理想.)

应该说明一下,上面关于理想 I 所加的条件,例如 $\bigcap_{n=1}^{\infty} I^n = \{0\}$ 并不是必需的.就是说,不满足这个条件也可以如上去作 $\overline{C}$. 我们对 I 作上述要求,使得更容易想象并容易和数学分析中类比.

上面介绍的方法虽是从有理数构造实数得到的启示,但却不能返回去用到有理数域的情形(无论如何 $\mathbb{Q}$ 是除 0 和本身外没有真理想的).这并不使人遗憾:我们乐于看到从旧方法中得到另一种格调的方法.

例 1　在整数环 $\mathbb{Z}$ 中取定理想 $I = (p)$, p 是一个素数.显然 I 符合我们上面的要求.$\mathbb{Z}$ 的 (p) - 进完备环 $\mathbb{Z}_{(p)}$ 称为 p - 进整数环.如果取定整数 α_n, $0 \leqslant \alpha_n < p$,　$n = 0,1,2,\cdots$ 而作序列 $\{a_n\}$, 其中正整数

$$a_n = \alpha_0 + \alpha_1 p + \alpha_2 p^2 + \cdots + \alpha_n p^n,$$

易见 $\{a_n\}$ 是一个 (p) - 进 Cauchy 序列.如果把序列 $\{a_n\}$ 写成级数形式,这就是

$$x = \alpha_0 + \alpha_1 p + \alpha_2 p^2 + \cdots + \alpha_n p^n + \cdots \quad 0 \leqslant \alpha_n < p. \tag{7}$$

我们还知(略去讨论) p - 进整数环 $\mathbb{Z}_{(p)}$ 中的元素或本身可表成(7)或其负元可表示成(7).而两个 p - 进整数(7)和

$$y = \beta_0 + \beta_1 p + \beta_2 p^2 + \cdots + \beta_n p^n + \cdots \qquad 0 \leqslant \beta_n < p \tag{8}$$

的运算规则则按“p - 进位规则”进行,即

$$\begin{aligned} x + y &= (\alpha_0 + \beta_0) + (\alpha_1 + \beta_1)p + (\alpha_2 + \beta_2)p^2 + \cdots \\ &= \gamma_0 + \gamma_1 p + \gamma_2 p^2 + \cdots \qquad 0 \leqslant \gamma_n < p, \end{aligned} \tag{9}$$

$$\begin{aligned} x \cdot y &= \alpha_0\beta_0 + (\alpha_0\beta_1 + \alpha_1\beta_0)p + \cdots + (\textstyle\sum_i \alpha_i\beta_{n-i})p^n + \cdots \\ &= \delta_0 + \delta_1 p + \delta_2 p^2 + \cdots \qquad 0 \leqslant \delta_n < p. \end{aligned} \tag{10}$$

(9)中第二个等号的意思在于“逢 p 进位”,即若 $\alpha_0 + \beta_0 > p$ 时 $\alpha_0 + \beta_0 = 1 \cdot p + \gamma_0$, 这时 $x + y = \gamma_0 + (\alpha_1 + \beta_1 + 1)p + \cdots$, 然后再考虑 $(\alpha_1 + \beta_1 + 1)$ 是否大于 p, 这样继续进行下去.(10)的第二个等号的意思类似.

现在来看看从实数域到复数域的构造对我们有什么启发.开始出现虚数,人们长期不敢承认.后来 C.F.Gauss (1777 - 1855)对复数给了一个几何上的解释——向量表示.于是逐渐大家接受了.有趣的也是自然的是:一旦接受了,很快就有人想到,既然能得到复数域,为什么不能再把数系扩大一些,找出更

多更好的数系呢？就这样，探索工作开始，直到 W.R.Hamilton (1805－1865) 成功迈出第一步.然而也是这一步，一方面结束了再扩大数系的探索，另一方面也开辟了代数研究中的一个方向——超复数系(现在的名词是"有限维代数").

可以这样来看复数域 $\mathbb{C}$：$\mathbb{C}$ 是实数域 $\mathbb{R}$ 上的二维向量空间，以 1 和 i 为基元素，1 和 i 的乘法表是：$1\cdot 1=1, 1\cdot i=i\cdot 1=i, i\cdot i=-1$，而任意两个元素 $x=a\cdot 1+b\cdot i, y=c\cdot 1+d\cdot i, a,b,c,d\in\mathbb{R}$，的乘法规则就是把基元素的乘法"线性扩充"一下，即

$$x\cdot y=(a\cdot 1+b\cdot i)(c\cdot 1+d\cdot i)$$
$$=ac\cdot(1\cdot 1)+ad\cdot(1\cdot i)+bc\cdot(1\cdot i)+bd\cdot(i\cdot i).$$

同样地，如果我们取任意域 F 上一个 n 维空间 A，它以 $x_1,\cdots,x_n$ 为基，并给出基元素 $x_1,\cdots,x_n$ 间的一个乘法表：

$$x_i\cdot x_j=\alpha_{i,j,1}x_1+\alpha_{i,j,2}x_2+\cdots+\alpha_{i,j,n}x_n,\quad \alpha_{i,j,k}\in F,\qquad(11)$$

再把基元素的乘法表(11)线性扩充到整个 F－空间 A，即规定

$$x\cdot y=(\sum_i\beta_i x_i)\cdot(\sum_j\gamma_j x_j)=\sum_{i,j}(\beta_i\gamma_j)(x_i\cdot x_j),$$

这样 F－空间 A 就有了一个乘法.如果基元素 x_i 之间的乘法满足结合律，即有 $\forall\ i,j,k,(x_ix_j)x_k=x_i(x_jx_k)$，不难证明这个 A 的乘法也满足结合律，如果基元素的乘法是交换的，A 的乘法也是交换的.直接验证可得 $(A,+,\cdot)$ 是一个环，这里的 + 当然是指 F－空间 A 中的加法.

例 2 四元数代数(Hamilton).设 H 是实数域 $\mathbb{R}$ 上的四维向量空间，取其一个含 1 的基，记作 $1,i,j,k$.规定基元素的乘法表如下：

	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

从表中可读出，例如 $ij=k, ji=-k$ 等等，从表上还可看出 $i^2=j^2=k^2=-1$.今把基元素的乘法和上面一样线性扩充到 H 上.直接验证可知，基元素之间的乘法适合结合律，例如 $(ij)k=kk=-1,\quad i(jk)=ii=-1$；$(ij)i=ki=j,\quad i(ji)=i(-k)=-(ik)=-(-j)=j$.这样就得到 $(H,+,\cdot)$ 是一个环，是一个非交换环，其单位元是 1.称 H 为四元数代数.容易看到 H

的子环 $\{\alpha\cdot 1+\beta\cdot i,\alpha,\beta\in\mathbb{R}\}$，$\{\alpha\cdot 1+\beta\cdot j,\alpha,\beta\in\mathbb{R}\}$，$\{\alpha\cdot 1+\beta\cdot k,\alpha,\beta\in\mathbb{R}\}$ 都和复数域是同构的.

今证 H 的非 0 元素都有逆元. 为此和复数类似，我们引入四元数的共轭数和模数的概念. 设四元数 $x=\alpha+\beta i+\gamma j+\delta k$，称 $\bar{x}=\alpha-\beta i-\gamma j-\delta k$ 为 x 的共轭四元数，易见

$$\overline{xy}=\bar{y}\cdot\bar{x},\quad \overline{x+y}=\bar{x}+\bar{y},$$
$$x\bar{x}=\bar{x}x=\alpha^2+\beta^2+\gamma^2+\delta^2.$$

称非负实数 $n(x)=x\bar{x}=\bar{x}x$ 为四元数 x 的模数. 显然 $x\neq 0$，则 $n(x)>0$，因而有

$$x\cdot\left(\frac{1}{n(x)}\bar{x}\right)=\left(\frac{1}{n(x)}\bar{x}\right)\cdot x=1,$$

即任意非 0 四元数有逆元.

我们知道，一个有 1 的交换环，若每一非 0 元有逆元，则称为域. 一个有 1 的(不一定是交换)环，若每一非 0 元有逆元，将称之为除环. 这样四元数代数是一个除环，也是历史上第一个除环的例子.

上面称 H 为四元数代数是有下面的原因. 对于通常环 $(R,+,\cdot)$，$(R,+)$ 只是一个加群，即交换群，而四元数代数 $(H,+,\cdot)$ 中，$(H,+)$ 还是 $\mathbb{R}$ - 向量空间. 由于 $\mathbb{R}$ - 向量空间，或者任意域上的向量空间都是有基，任一元素都可表成基元素的线性组合，这说明向量空间的结构比交换群的结构简单很多. 对这种其加群是向量空间的环值得给一个特殊的名字.

定义 2.6　$(A,+,\cdot)$ 是一个环. 如果

A1) $(A,+)$ 是域 F 上的向量空间；

A2) $\forall\ \alpha\in F, x,y\in A, \alpha(xy)=(\alpha x)y=x(\alpha y)$.

则称 A 为域 F 上代数. 当 $(A,+)$ 是域 F 上有限维向量空间时，则称 A 为域 F 上有限维代数. 当 $(A,+,\cdot)$ 是除环时，称 A 为 F 上可除代数.

易见四元数代数 H 是实数域 $\mathbb{R}$ 上的四维代数. 复数域是 $\mathbb{R}$ 上二维代数，而实数域是 $\mathbb{R}$ 上的一维代数.

下面定理(略去证明)说明扩大“好”数系的企图在此停下来的原因.

定理　(F.G. Frobenius (1849 - 1917))　实数域 $\mathbb{R}$ 上有限维可除代数有且只有下列三个：实数域 $\mathbb{R}$，复数域 $\mathbb{C}$ 和四元数代数 H.

人们希望我们的“数”，在作除法时是可行的而在作乘法时是可交换的. 否则在操作起来太不方便，“数”也就不成其为数了. 上述定理说满足这样要求的

数就该到复数域而止了.

但不是说四元数(以及后来的八元数(Cayley 数),后者的乘法已不是结合的了)是没有用的.它们在几何上是有用的.而四元数代数引出了本世纪初发展起来的环论的一个分支——有限维代数理论.

在本节最后我们给出作为环论支柱的一类例子——群代数.

例 3 设 G 是阶为 n 的群,其元素为 $e = g_1, g_2, \cdots, g_n$. 任取域 F 上的一个 n 维向量空间 A,并取它的一个基.显然此基由 n 个元素组成.我们当然可以用任意符号来表示这些基元素.这次就用群 G 的元素 $g_1, g_2, \cdots, g_n$ 表示这些基元素,并利用群 G 的乘法来规定向量空间 A 的这组基元素间的乘法,然后再把它线性扩充到整个空间 A 上去.这时易见由于群的乘法有结合律,故基元素之间的乘法满足结合律,因而 $(A, +, \cdot)$ 成为一个环.由于 $(A, +)$ 还是域 F 上的向量空间,故 $(A, +, \cdot)$ 是域 F 上 n 维代数.称之为群 G 在域 F 上的群代数,记作 $A = F[G]$.

例如,取 $F = \mathbb{Q}$, G 是 5 阶循环群 $\{a\}$. 此时 $\mathbb{Q}[G]$ 中的元素为 $\alpha_0 e + \alpha_1 a + \alpha_2 a^2 + \alpha_3 a^3 + \alpha_4 a^4$. $F[G]$ 中的乘法,例如

$$\begin{aligned}&(3e + 4a - 5a^2)(a^2 - a^4)\\&= (3a^2 - 3a^4) + (4a^3 - 4a^5) + (-5a^4 + 5a^6)\\&= (3a^2 - 3a^4) + (4a^3 - 4e) + (-5a^4 + 5a)\\&= -4e + 5a + 3a^2 + 4a^3 - 8a^4.\end{aligned}$$

又例如,取 $F = \mathbb{Q}$, G 为 Klein 四元群,即 G 由下列 $\{1,2,3,4\}$ 的置换组成:

$$e = 1, \quad a = (1\ \ 2), \quad b = (3\ \ 4), \quad c = (1\ \ 2)(3\ \ 4).$$

此时 $F[G]$ 中的元素可写成 $\alpha_0 + \alpha_1(1\ \ 2) + \alpha_2(3\ \ 4) + \alpha_3(1\ \ 2)(3\ \ 4)$,而其中乘法,例如有

$$\begin{aligned}&(3\cdot(1\ \ 2) - 2\cdot(3\ \ 4))(-1 + (1\ \ 2)(3\ \ 4))\\&= (-3\cdot(1\ \ 2) + 3\cdot(1\ \ 2)(1\ \ 2)(3\ \ 4)) +\\&\quad (2\cdot(3\ \ 4) - 2\cdot(3\ \ 4)(1\ \ 2)(3\ \ 4))\\&= (-3\cdot(1\ \ 2) + 3\cdot(3\ \ 4)) + (2\cdot(3\ \ 4) - 2\cdot(1\ \ 2))\\&= -5\cdot(1\ \ 2) + 5\cdot(3\ \ 4).\end{aligned}$$

练习

1. 设 R 是环,证明:如果 R 有左零因子,则存在 R 中非零元 x,使得 x 既是左零因子,又是右零因子.

2. 验证 $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ 对于数的加法与乘法构成整环.

3. 连续实函数环 $C[0,1]$ 不是整环.当 n 为合数时,$\mathbb{Z}_n$ 不是整环.

4. 求 $\mathbb{Z}[i]$ 的分式域.

5. 设 F 是数域,证明: F_n 对于矩阵的加法、乘法、数乘构成 F 上有限维代数.

§3 多项式环

这里我们继续由已知环来构造新环的工作.上一节是利用数系扩张的经验来构造新环或域.本节来构造环上的矩阵环和多项式环.矩阵、多项式以及现在我们讨论的群、环、域等代数系统,都是数的延伸,都是由于刻画几何量和物理量的需要而诞生和发展的.由于要刻画的对象,几何量和物理量,愈来愈复杂,普通的数已不够用了.例如群的出现是应刻画对称性而出现的.因而把这些行之有效的基本对象,诸如数环或域以及其上的矩阵、多项式环作推广是自然而必要的.

设 R 是有 1 的环.在前面的例子中我们已经介绍以数环 F 中元素 a_{ij} 作系数的 $n\times n$ 矩阵 (a_{ij}),关于矩阵的乘法和加法作成的 n 阶矩阵环 $M_n(F)$.我们可将矩阵中的元素从数环推广到一般的环.记环 R 上的 $n\times n$ 矩阵关于矩阵的加法和乘法所成的 n 阶矩阵环记为 $M_n(R)$.这种推广没有任何困难,原因是矩阵 (a_{ij}) 是一个形式.

设 R 是有 1 的环.考虑以 R 中元素 a_i 作系数的多项式,也就是形如

$$a_0+a_1x+a_2x^2+\cdots+a_nx^n,\quad a_i\in R \tag{1}$$

的表达式.如果把(1)理解为以 R 为定义域,以 R 为值域的多项式函数,亦即

$$\phi: R\longrightarrow R$$

$$x\longmapsto a_0+a_1x+\cdots+a_nx^n.$$

这时令 $R[x]$ 表示这些 R 上多项式函数的全体,容易知道 $R[x]$ 关于函数的加法和乘法作成一个环.当然函数环 $R[x]$ 中的两个元素,例如(1)和

$$b_0+b_1x+b_2x^2+\cdots+b_mx^m,\quad b_i\in R, \tag{2}$$

它们相等的定义是:

$$a_0+a_1x+\cdots+a_nx^n=b_0+b_1x+\cdots+b_mx^m$$

$$\Longleftrightarrow \forall\ c\in R, a_0+a_1c+\cdots+a_nc^n=b_0+b_1c+\cdots+b_mc^m. \tag{3}$$

当 R 是数环或数域时,我们知道一个 n 次多项式最多有 n 个不同的根,故(3)等价于

$$a_0+a_1x+\cdots+a_nx^n=b_0+b_1x+\cdots+b_mx^m$$

$$\Longleftrightarrow n=m \text{ 且 } \forall\, i, a_i=b_i. \tag{4}$$

(4)是一个定理,这是当 R 是数环时,多项式函数环 $R[x]$ 中的一个定理.但当 $R=\mathbb{Z}_5=\{0,1,2,3,4\}$ 时,在多项式函数环 $\mathbb{Z}_5[x]$ 中,依定义(3)我们有

$$x + x(x-1)(x-2)(x-3)(x-4) = x,$$

这里由(4)所表达的事实当然不成立，即 $\mathbb{Z}_5[x]$ 中是没有定理(4)的. 这种现象是我们不喜欢的：应该说(4)是多项式的"命根子"，不管是作为定理还是作为定义，我们总希望(4)成立.

这就引出了关于(1)的形式观点. 形式就是没有实际内容的符号，留待我们赋予它内容，但形式(1)会引起麻烦：其中的" + "和以后将定义的加法有关系吗？x^2 是两个 x 相乘吗？a_1x 是 a_1 和 x 相乘吗？然而乘法我们尚未定义，因而建立多项式的形式观点，要进行某种处理. 其想法是很简单的，就如同作分式域时用纯形式 (a,b) 来代替我们心目中的 ab^{-1} 是一样的.

我们来构造 R 上多项式形式环，其中 R 是已知的有 1 的环.

用 P 表示下列符号——用括号括起来的无穷序列的全体：

$$(a_0, a_1, a_2, \cdots) \quad a_i \in R, \tag{5}$$

其中，a_i，$i = 0,1,2,\cdots$，中最多只有有限个元素非零. 我们规定 P 中两个元素(5)和

$$(b_0, b_1, b_2, \cdots), \quad b_i \in R \tag{6}$$

相等当且仅当对任意 i，有 $a_i = b_i$. 在集 P 中规定加法、乘法如下：

$$(a_0, a_1, \cdots) + (b_0, b_1, \cdots) = (a_0 + b_0, a_1 + b_1, \cdots), \tag{7}$$

$$(a_0, a_1, \cdots) \cdot (b_0, b_1, \cdots) = \left(a_0b_0, a_0b_1 + a_1b_0, \cdots, \sum\nolimits_{i=0}^{n} a_ib_{n-i}, \cdots\right). \tag{8}$$

直接验证(请读者至少证明一下乘法的结合律)可知 $(P, +, \cdot)$ 是一个环，其零元是 $(0,0,\cdots,0,\cdots)$ 而单位元是 $(1,0,\cdots,0,\cdots)$.

我们大家都清楚上面引入集 P，P 中元素的相等，P 中的加法和乘法的背景. 下面如在作分式域时最后又把 (a,b) 还原为 ab^{-1} 一样，我们把环 P 设法表成我们习惯的多项式环的样子.

我们再引入符号 x，而规定

$$x = (0,1,0,\cdots),$$
$$a = (a,0,\cdots).$$

这时在环 $(P, +, \cdot)$ 中有

$$x^2 = (0,0,1,0,\cdots),$$
$$x^n = (0,\cdots,0,1(\text{第 } n+1 \text{ 个位置}),0,\cdots),$$

$a \cdot b$(环 P 中的乘法) $= ab$(环 R 中的乘法),

$$ax^n = (0,\cdots,0,a(\text{第 } n+1 \text{ 个位置}),0,\cdots).$$

一般地有

$$a_0 + a_1x + \cdots + a_nx^n = (a_0,a_1,\cdots,a_n,0,\cdots). \tag{9}$$

这样 $P = \{a_0 + a_1x + \cdots + a_nx^n, a_i \in R\}$ 而 P 中元素的相等,加法(7),乘法(8),根据 P 中元素表达形式的转换式(9),就变成

$$a_0 + a_1x + \cdots + a_nx^n = b_0 + b_1x + \cdots + b_mx^m$$

$$\Longleftrightarrow n = m \text{ 且 } \forall\ i, a_i = b_i, \tag{10}$$

$$(a_0 + a_1x + \cdots + a_nx^n) + (b_0 + b_1x + \cdots + b_mx^m)$$

$$= (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_k + b_k)x^k, \tag{11}$$

其中 $k = \max(n,m)$ 而认定 $a_i = 0, i > n, b_j = 0,\ j > m$.

$$(a_0 + a_1x + \cdots + a_nx^n) \cdot (b_0 + b_1x + \cdots + b_mx^m)$$

$$= a_0b_0 + (a_0b_1 + a_1b_0)x + \cdots$$

$$+ \left(\left(\sum_{i=0}^{n} a_ib_{k-i}\right)\right)x^k + \cdots + a_nb_mx^{n+m}. \tag{12}$$

也就是我们熟悉的多项式的相等和运算规则.

定义 3.1 设 R 是有 1 的环.将把如上定义的环 P 称为环 R 上一元多项式形式环,常简称为 R 上一元多项式环,仍记作 $R[x]$,并称 x 为 R 上不定元.

今后我们谈论一元多项式环 $R[x]$,都是在形式观点下,即都是指一元多项式形式环.

对数环 R 言,我们已经看到 R 上一元多项式环函数环和 R 上一元多项式形式环是一致的,即是同构的,因而对数环言,我们不必区分多项式函数环和多项式形式环,只是在这里再强调一下:(4)或(10)对多项式函数环是定理,而对多项式形式环是定义.事实上根据下面命题,对于无限整环,即含有无限多个元素的整环 R,对这两种观点也不必区分.

引理 3.2 设 R 是整环. $p(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$. 若 $p(b_i) = 0,\quad i = 1,2,\cdots,m \leqslant n$,且 b_i 彼此不同,则 $p(x) = (x - b_1)\cdots(x - b_m)g(x)$,其中 $g(x) = c_0 + c_1x + \cdots + a_nx^{n-m}$.

当 R 是交换环时,$R[x]$ 也是,当 R 无零因子时,$R[x]$ 也无零因子.此时在 $R[x]$ 中有因子分解式: $x^m - b^m = (x - b)(x^{m-1} + bx^{m-2} + \cdots + b^{m-2}x + b^{m-1})$. 我们把此引理的详细证明留给读者去完成.

命题 3.3　设 R 是无限整环. R 上一元多项式函数环 $R[x]^*$ 和 R 上一元多项式(形式)环 $R[x]$ 是同构的.

证明　只需证明在函数环 $R[x]^*$ 中(4)成立就够了.说得详细一点,设

$$\phi:\quad R[x] \longrightarrow R[x]^*$$
$$a_0 + a_1x + \cdots + a_nx^n \longmapsto a_0 + a_1x + \cdots + a_nx^n.$$

由于在形式环 $R[x]$ 中元素的表示法是唯一的,故 ϕ 是一个映射.易知 ϕ 是保持运算的,即 ϕ 是环 $R[x]$ 到环 $R[x]^*$ 的同态.事实上,它是满同态.显然

$$\mathrm{Ker}\phi = \{p(x) = a_0 + a_1x + \cdots + a_nx^n \mid \text{对任意 } b \in R,$$
$$p(b) = a_0 + a_1b + \cdots + a_nb^n = 0\},$$

因而要证明命题,只需证明 $\mathrm{Ker}\phi = \{0\}$,这就是只需证:若对任意 $b \in R$,如果 $p(b) = a_0 + a_1b + \cdots + a_nb^n = 0$,则对任意 $i, a_i = 0$.

用反证法而设 $a_n \neq 0$. 由于 R 是无限集,可取出 $n+1$ 个不同元素 $b_1, \cdots, b_n, c$. 由引理 3.2 知 $p(x) = (x - b_1)\cdots(x - b_n)\cdot a_n$. 再由 $0 = p(c) = (c - b_1)\cdots(c - b_n)\cdot a_n$,以及 $c - b_i \neq 0$ 而 R 中无零因子,便得 $a_n = 0$. 这与假设矛盾.故命题得证.□

这样我们完成了 R 上一元多项式环 $R[x]$ 的构造,并明确了关于多项式的两种观点,知道什么时候这两种观点一致,什么时候(例如 R 是有限域时)两者不一致.应该说,这里的重要而具体的成果是,对于有限域 F 在式(10),(11),(12)的定义下我们有一个一元多项式环 $F[x]$.

有了 R 上一元多项式环 $R[x]$,考虑 $R[x]$ 上的一元(y)多项式环 $R[x][y]$,把它记作 $R[x,y]$,即 $R[x,y] = R[x][y]$,称之为 R 上二元多项式环,而称 x,y 为 R 上二个无关的不定元.易见 $R[x,y] = R[x][y]$ 中的元素形状为

$$p_0(x) + p_1(x)y + \cdots + p_n(x)y^n, \quad p_i(x) \in R[x].$$

若再把 $p_i(x)$ 写成 x 的多项式,并依分配律展开便得

$$\sum a_{ij}x^iy^j, \quad a_{ij} \in R.$$

这就是 x,y 的多项式.称 x^iy^j 为单项式,而 a_{ij} 为其系数.两个 x,y 的多项式 $f(x,y), g(x,y)$ 相等当且仅当它们有相同的形式:具非零系数的单项式完全一样且相应的系数相等.

应用数学归纳法,可定义 R 上 $n+1$ 元多项式环

$$R[x_1, \cdots, x_n, x_{n+1}] = R[x_1, \cdots, x_n][x_{n+1}],$$

而称 $x_1, \cdots, x_{n+1}$ 为 R 上 $n+1$ 个无关的不定元. m 元多项式的表达式,单项式,两个 m 元多项式的相等,等等,完全和二元情形类似.域 F 上多元多项式

环是特别重要的一类环.我们将在附录中去介绍它.

下面再介绍一个由一些已知环来构造新环的方法.它和群的外直积的概念是类似的.

设 $R_i, i \in \mathbb{Z}^+$ 是环.考虑如下的无限长形式向量:

$$(r_1, r_2, \cdots, r_i, \cdots)$$

在 i - 分量处的元素 $r_i \in R_i$.

令 R 表示所有这样向量的全体.规定 R 中的两个元素相等当且仅当它们完全一样.再规定 R 的加法和乘法按分量进行,即

$$\begin{aligned}
&(r_1, r_2, \cdots, r_i, \cdots) + (r'_1, r'_2, \cdots, r'_i, \cdots) \\
=&(r_1 + r'_1, r_2 + r'_2, \cdots, r_i + r'_i, \cdots), \\
&(r_1, r_2, \cdots, r_i, \cdots) \cdot (r'_1, r'_2, \cdots, r'_i, \cdots) \\
=&(r_1 r'_1, r_2 r'_2, \cdots, r_i r'_i, \cdots).
\end{aligned}$$

则易见 $(R, +, \cdot)$ 是一个环.称之为环 R_i, $i \in \mathbb{Z}^+$ 的直积,记作 $\prod_{i \in \mathbb{Z}^+} R_i$.

关于域 F 上多项式环 $F[x]$,我们作进一步讨论.

对加群 $(F[x], +)$ 再引入数乘运算:$a \in F, p(x) = a_0 + a_1 x + \cdots + a_n x^n \in F[x]$,规定

$$a \cdot p(x) = aa_0 + aa_1 x + \cdots + aa_n x^n.$$

容易验证,这时加群 $(F[x], +)$ 就成为域 F 上的向量空间,而($F[x], +, \cdot$, 数乘)就成为 F 上代数.这时也就称 $F[x]$ 为域 F 上多项式代数.

显然 F 上向量空间($F[x]$, +, 数乘)不是有限维的.

说域 F 上的一个向量空间 V 的一个子集(有限或无限) B 是 F 上线性无关的,如果 B 的任意有限子集都是 F 上线性无关的.称 V 的一个子集 B 是向量空间 V 的一个基,如果

1) B 是 F 上线性无关集,

2) V 中任一元素 x 都可表示成 B 的某个有限子集 B_x 的线性组合.

可以看出,这是有限维空间的基的概念向任意向量空间的推广.

按照这个定义,域 F 上的向量空间 $F[x]$ 有一个基,它由无限多个元素 $1, x, x^2, \cdots$ 组成:$B = \{1, x, x^2, \cdots\}$ 是 F 上线性无关集,这是因为对任意 n,

$$a_0 \cdot 1 + a_1 \cdot x + a_2 \cdot x^2 + \cdots + a_n \cdot x^n = 0, \quad a_i \in F$$

当且仅当 $\forall\ i, a_i = 0$. 另一方面, $F[x]$ 中任一元素(多项式)显然可以表示成 B 的某个有限子集的线性组合.这就证明了 B 是 F 上向量空间 $F[x]$ 的一个基.这样 F 上多项式代数 $F[x]$ 可以看成

1) $B = \{1, x, x^2, \cdots\}$ 是域 F 上向量空间 $F[x]$ 的一个基，

2) 基元素之间的乘法表是：$x^i \cdot x^j = x^{i+j}$，　$i, j \in \mathbb{Z}^+ \cup \{0\}$，其中 $x^0 = 1$.

无论是把有限群的所谓群代数的构造方法直接推广到无限群的情形，还是上面这个多项式代数的例子给我们的启发，我们都会使用下面这个构造环或代数的方法：设 F 是一个域，而 S 是一个半群. 把 S 当作基而得到一个 F 上向量空间，把它记作 $F[S]$，这就是说，$F[S]$ 中元素都可写成

$$a_1 s_{i_1} + a_2 s_{i_2} + \cdots + a_n s_{i_n}, \quad a_i \in F, s_{i_j} \in S, s_{i_j} \text{ 彼此不同}$$

的形式，而两个这种形状的元素相等当且仅当，除系数为 0 的项以外，它们具有完全一样的形式. 我们就按照半群 S 中的乘法来规定向量空间 $F[S]$ 的基 S 中元素之间的乘法，然后再把这个基元素之间的乘法按照分配律而扩大成 $F[S]$ 中任意两个元素之间的乘法. 由于半群 S 的乘法适合结合律，易知 $F[S]$ 的这个乘法也适合结合律. 经过验证可知（$F[S]$，+，·，数乘）成为域 F 上的一个代数，将称之为关于半群 S 的半群代数.

和前面构造有限群 G 的群代数相比较，唯一的不同处就是那里利用有限集 G 作一个 F 上以 G 为基的有限维空间，而这里是用 S（有限或无限）作一个以 S 为基的向量空间.

如果这里的半群 S 就是一个有限群，则这里的构造和过去的构造就完全一样了. 取 S 为 n 个元素 $x_1, x_2, \cdots, x_n$ 生成的自由交换半群 $\{1$(空字)，$x_1^{m_1} x_2^{m_2} \cdots x_n^{m_n}$，　$m_i \in \mathbb{Z}^+ \cup \{0\}$ 且至少有一 $m_j \neq 0\}$，则 $F[S]$ 就是域 F 上的 n 元多项式代数.

如果取 S 为 n 个元素 $x_1, \cdots, x_n$ 生成的自由半群，则称 $F[S]$ 为 n 元自由代数，常记作 $F\langle x_1, \cdots, x_n\rangle$. 例如 $F\langle x, y\rangle$ 的元素是 x, y 的“不交换多项式”，如 $xyx^2 - y^2xy^2$ 等等.

结束一般环构造的介绍，我们简单回顾并综合利用一下这里介绍的方法.

由已给环的子环和商环我们可以获得许多新的环. 再和作分式域，作 I - 进完备环，作群代数，作矩阵环，作多项式环等构造方法结合起来，就会得更多的环，从而丰富我们对环的认识，也扩大环的表现力及应用. 下面简略提一下不准备深入讨论的环，详细推导留给感兴趣的读者.

整数环 $\mathbb{Z}$ 中取理想 $I = (p)$，　p 是素数，作 I - 进完备环便得 p - 进整数环 $\mathbb{Z}_{(p)}$. 它是一个整环，它的元素 p - 进整数可写成

$$a_0 + a_1 p + a_2 p^2 + \cdots + a_n p^n + \cdots, \quad a_i \in \{0, 1, 2, \cdots, p-1\}$$

的形状. 作 p - 进整数环 $\mathbb{Z}_{(p)}$ 的分式域，便得 p - 进数域，它的元素可写成

$$a_t p^t + a_{t+1} p^{t+1} + \cdots + a_n p^n + \cdots,\ a_i \in \{0,1,2,\cdots,p-1\},$$

其中 $t \in \mathbb{Z}$，即有的是从 p 的负幂项开始，因而保证每一非零元都有逆元.

类似地，在域 F 上的多项式环 $F[x]$ 中取理想 $I=(x)$，作 I - 进完备环便得域 F 上形式幂级数环 $F[[x]]$. 它是一个整环，它的元素形式幂级数可写成

$$a_0 + a_1 x + \cdots + a_n x^n + \cdots,\quad a_i \in F$$

的形状. 作 $F[[x]]$ 的分式域，便得形式分幂级数域，它的元素，通常称作形式 Lorentz 幂级数，可写成

$$a_t x^t + a_{t+1} x^{t+1} + \cdots + a_n x^n + \cdots,\quad a_i \in F,$$

其中 $t \in \mathbb{Z}$，即可能从 x 的负幂项开始，因而保证每一非零元都有逆元. 如果，从域 F 上多项式 $F[x]$ 出发直接作分式域，便得有理分式域，其元素可表为有理式 $P(x)/Q(x)$，其中 $Q(x)$ 是非零多项式，即至少有一个非零系数的多项式.

练习

1. 在 $\mathbb{Z}_7[x]$ 中计算：

$$([3]x^2+[5]x+[4])([4]x^2+[2]x+[3]).$$

2. 设 H 是四元数代数，
   1) 作为 H 上多项式有 $x^2+1=(x+i)(x-i)$；
   2) 作为 H 上的函数，有 $x^2+1 \neq (x+i)(x-i)$.
3. 设 R 是整环，则 $R[x]$ 也是整环.
4. 在 $M_2(\mathbb{Z})$ 中，定义

$$T=\left\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \middle| a,b,c \in \mathbb{Z}\right\},\quad I=\left\{\begin{pmatrix} 0 & 2d \\ 0 & 0 \end{pmatrix} \middle| d \in \mathbb{Z}\right\}.$$

   1) 证明：T 是 $M_2(\mathbb{Z})$ 的子环；
   2) 证明：I 是 T 的理想；
   3) T/I 是由哪些元素组成的？
5. 设 R 是有单位元的交换环，$D(R)$ 是 $M_n(R)$ 中所有对角矩阵的集合，$C(D(R))$ 是 $M_n(R)$ 中与 $D(R)$ 中元素可交换的矩阵的全体，求证：
   1) $D(R)$ 是 $M_n(R)$ 的子环；
   2) $C(D(R))=D(R)$.

§4　交换环

群论可粗分为四大块：有限群论、交换群论、无限群论以及具有各种几何

结构(拓扑结构、解析结构、代数几何结构)的群(拓扑群、Lie 群、代数群等). 结合环论则可粗分为三大块:交换环、非交换环以及带有各种结构(序结构、几何结构)的环. 在这个介绍群、环、域、模的基本概念的课程中,我们将着重讲交换环. 在谈论交换环时,要常想着整数环、二次数环(见 §5)、多项式环以及函数环这些基本例子,我们将把研究的对象限制在整环上,上面提到的例子除函数环外都属于整环的范围.

本节中 R 将永远表示整环.

首先研究一下整环 R 的加法群.

可以把环 A 想作是由一个加群 A 再引入一个乘法而得到的. 对任意给的加群 A,引入零乘,即规定: $\forall\ x,y\in A, xy=0$, 这显然得到一个环. 然而本质上和加群没有什么不同:它的乘法不给我们了解 A 带来任何新的信息. 下面将看到,并非对于任意的加群,都可以定义乘法而使它成为整环.

对整环 R 有下面情形:一是对任意 $n\in\mathbb{Z}^+$, n 个 1 相加都不是零,即 1 的阶是 ∞. 这时任意 $0\neq a\in R$, 任意 n 个 a 相加也不是 0,因为若 $0=na=a+\cdots+a=n\cdot a$, 由于 $a\neq 0$ 及乘法消去律成立,该有 $n=0$, 而这是与假设矛盾的. 因而在这种情形下,加群 $(R,+)$ 的每一非零元的阶都是 ∞.

另一种情形是存在一 $n\in\mathbb{Z}^+$, 在加群 $(R,+)$ 中 $n=0$, 即 1 的阶是有限的,设其阶为 $n>1$. 若 n 非素数,则 $0=n=n_1\cdot n_2$, 在整环 R 中有乘法消去律,故 $n_1=0$ 或 $n_2=0$, 但 n_1,n_2 小于 n, 这和 1 的阶为 n 是矛盾的. 故在这种情形,1 的阶为素数 p, 随之,与上类似地可得加群 $(R,+)$ 中任意非零元素 a 的阶都等于素数 p.

总结一下就是下面

命题 4.1 R 是有 1 整环,则

a) 加群 $(R,+)$ 中所有非零元有相同的阶,或者是 ∞, 或者是素数 p.

b) R 或含整数环 $\mathbb{Z}$ 为其子环,或含有限域 $\mathbb{Z}_p$ 为其子环.

证明 b)成立是因为,当单位元 1 的阶为 ∞ 时,1 生成的子环 $\langle 1\rangle\cong\mathbb{Z}$, 而当单位元 1 的阶为素数 p 时, $\langle 1\rangle\cong\mathbb{Z}_p$. □

定义 4.2 称整环 R 的加群 $(R,+)$ 的非零元素的公共阶为 R 的特征.

由上知, R 的特征或为 ∞ 或为素数 p.

上面的讨论说明,由于整环 R 的乘法有交换律和消去律,因此对 R 的加法有一些限制.

命题 4.3 a) 特征为 ∞ 的域含有理数域 $\mathbb{Q}$ 为其子域;

b) 特征为素数 p 的域含有限域 $\mathbb{Z}_p$ 为其子域. □

由于我们有上命题,故有下面的

定义 4.4　称 $\mathbb{Q}$ 及 $\mathbb{Z}_p$，p 是素数，为素域．这样特征为 ∞ 的素域就是有理数域 $\mathbb{Q}$，而对一素数 p 有唯一特征 p 的素域，这就是 $\mathbb{Z}_p$．

现在讨论整环 R 的子环，理想和商环．

R 的带 1 的子环 A 当然还是整环，因为乘法的交换律和消去律对整个 R 成立，当然对 R 的一部分 A 也是成立的．

但 R 的商环 R/I 就不一定是整环了，而问题是出在乘法消去律上．

这里再来概括一下环 R 和商环 $\overline{R} = R/I$ 的异同：R 的元素是 x，$\overline{R}$ 的元素是 $\bar{x} = x + I$；运算的规则是"一样"的，$\bar{x} \cdot \bar{y} = \overline{xy}$，$\bar{x} + \bar{y} = \overline{x + y}$，但相等的关系不一样，$x = y$ 当然 $\bar{x} = \bar{y}$，但 $x \neq y$，也可能有 $\bar{x} = \bar{y}$．$\bar{x} = \bar{y}$ 当且仅当 $x - y \in I$，特别 $\bar{x} = \bar{0}$ 当且仅当 $x \in I$．

例如，域 F 上多项式环 $F[x,y]$ 是整环，但商环 $F[x,y]/(xy)$ 便不是，因为 $\bar{x} \neq 0$，$\bar{y} \neq 0$ 而 $\bar{x} \cdot \bar{y} = \overline{xy} = \bar{0}$．

保证 R/I 是整环的理想 I 该是什么样子？这从上面关于商环的说明以及例子可以想到，理想 I 该有性质：若 $x \notin I$　$(\bar{x} \neq 0)$，$y \neq\in I$　$(\bar{y} \neq 0)$，则 $xy \notin I$　$(\overline{xy} \neq 0)$，或等价地，若 $xy \in I$，则 x, y 中至少有一个属于 I．

定义 4.5　称交换环 A 的理想 I 为素理想，如果 $I \neq A$ 且 $xy \in I$，必有 x 或 y 属于 I，或等价地，$x \notin I$，$y \notin I$ 则 $xy \notin I$．

请读者把交换环的素理想和整数环 $\mathbb{Z}$ 的素数或多项式环 $F[x]$ 中的不可约多项式比较一下，你会对素理想多一点感性认识．

定理 4.6　设 A 是有 1 交换环，I 是 A 的理想．则 A/I 是整环当且仅当 I 是素理想．

证明　设 $\overline{A} = A/I$ 是整环．在 A 中任取元素 $x \notin I$，$y \notin I$，则在 $\overline{A}$ 中 $\bar{x} \neq \bar{0}$，$\bar{y} \neq \bar{0}$．由于 $\overline{A}$ 是整环，故 $\bar{0} \neq \bar{x} \cdot \bar{y} = \overline{xy}$，此式说明 $xy \notin I$，即证得 I 是素理想．

反之，设 I 是素理想．在 $\overline{A}$ 中任取元素 $\bar{x} \neq \bar{0}$，$\bar{y} \neq \bar{0}$，而往证 $\bar{x} \cdot \bar{y} \neq \bar{0}$．$\bar{x} \neq \bar{0}$，$\bar{y} \neq \bar{0}$ 意味着 $x \notin I$，$y \notin I$．但 I 是素理想，由之可得 $xy \notin I$，这就是 $\overline{xy} \neq \bar{0}$．即证得 $\overline{A}$ 是整环．□

现在我们进而问：保证 R/I 是域的理想 I 是什么样子？

为此先作一点准备．易知域 F 的理想只有 (0) 和 F 本身．反过来，我们有

命题 4.7　设 A 是有 1 的交换环，如果 A 除了 (0) 和 A 外没有其它理想，则 A 必是域．

证明 这就是要证 A 的非零元 a 必有逆元. 易知 $aA = Aa$ 是环 A 的一个理想. 由于 A 有单位元 1,故 $0 \neq a = a \cdot 1 \in aA$, 即 $aA \neq (0)$. 依假设该有 $aA = A$. 再由于 $1 \in A$, 故有 $b \in A$ 使 $ab = 1$, 即 a 有逆元 b. □

上面命题中假设 A 有单位元是本质的,就是说,去掉这个假设命题就不成立了. 这只要想一下素数 p 阶循环群 A 上的零乘环就可明白了.

希望 A/I 是一个域,就是要求在 I 和 A 之间不再有 A 的理想. 这就是下面定义的内容.

定义 4.8 一个环 A 的真理想 I 称作是 A 的极大理想,如果不存在 A 的理想 J 有 $I \subsetneq J \subsetneq A$.

"最大"和"极大"是两个不同的概念,"最大"是比谁都大,而"极大"是没有谁比它大. "最大"的最多只能有一个,而"极大"的却可以有很多. 例如在整数环 $\mathbb{Z}$ 中,素数 p 生成的理想 (p) 都是极大理想. 这是因为,如果 $(p) \subsetneq J$, 则 J 中必有整数 n, 它不是 p 的倍数,即 p, n 互素,因此有 s, t 使得 $1 = sp + tn \in J$, 随之 $J = \mathbb{Z}$. 这就证得 (p) 是 $\mathbb{Z}$ 的极大理想,它们的个数是无限多. 当然它们中谁也不是"最大"的.

定理 4.9 设 A 是有 1 的交换环, I 是 A 的理想. 则 A/I 是域当且仅当 I 是 A 的一个极大理想.

证明 由上面命题 4.7,我们为此要证明的就是: $\overline{A} = A/I$ 没有真理想当且仅当 I 是 A 的一个极大理想. 由前面的关于环的同态定理,我们知道,在介于 I 和 A 之间的 A 的理想集 $\Sigma = \{A \text{ 的理想} J \mid I \subsetneq J \subsetneq A\}$ 和 $\overline{A}$ 的真理想集 $\overline{\Sigma} = \{\overline{A} \text{ 的真理想} \overline{J} \mid \overline{0} \subsetneq \overline{J} \subsetneq \overline{A}\}$ 之间有一个一一对应 θ:

$$\theta: \Sigma \longrightarrow \overline{\Sigma}$$

$$J \longmapsto \overline{J} = \{\overline{x} = x + I, x \in J\}.$$

请读者再重新证明一下这个事实. 根据这个事实,当 Σ 和 $\overline{\Sigma}$ 中有一个是空集时,另外一个也必定是空集,而这正是我们要证的. □

域当然是有 1 的整环,故由上面两个定理便得

命题 4.10 设 A 是有 1 的交换环. A 的极大理想必是 A 的素理想. □

下面看几个例子.

例 1 整数环 $\mathbb{Z}$. 下一节中我们将证明: $\mathbb{Z}$ 的每一个理想都是主理想,即是由某个整数 n 生成的理想 (n).

这样,若 n 不是素数,说是 $n = 6 = 2 \cdot 3$, 此时 $2 \notin (6)$, $3 \notin (6)$ 但 $2 \cdot 3 \in (6)$, 这说明 (6) 不是素理想,同理,当 n 不是素数时, (n) 也不是素理想. 若 p 是素数,上面已经看到, (p) 是极大理想,当然更是素理想. 这样在 $\mathbb{Z}$ 中

极大理想和素理想是等价的概念,它们就是(p),p是素数.

例 2 域F上一元多项式环$F[x]$. 和$\mathbb{Z}$一样,将证$F[x]$也是一个主理想整环,即每个理想都是主理想的整环.

若$p(x)$是不可约多项式,则$(p(x))$是一个极大理想(请读者自证),因而也是$F[x]$的素理想. 若$f(x)$不是不可约多项式,则和$\mathbb{Z}$情况一样,可知$(f(x))$不是素理想. 这样,在$F[x]$中极大理想和素理想是等价的概念,它们就是$(p(x))$,$p(x)$是不可约多项式.

例 3 容易看到$\mathbb{Z}[x]$中的理想(x)是一个素理想. 今考察由 2 和x生成的理想$(2,x)$,此理想中的元素为$2\cdot g(x)+x\cdot h(x)$,$g(x),h(x)\in\mathbb{Z}[x]$,即是常数项为偶数(包括 0)的整系数多项式. 若有理想I较之真大,则I中必有一常数项为奇数的整系数多项式,随之$1\in I$,因而$I=\mathbb{Z}[x]$. 这就说明$(2,x)$是一个极大理想. 这样由$(x)\subsetneq(2,x)$我们看到在$\mathbb{Z}[x]$中有的素理想不是极大理想.

一个自然的问题是,在有 1 的交换环A中是否必有素理想? 是否必有极大理想? 由于极大理想也是素理想. 因而可归成一个问题:极大理想的存在问题.

在本课程涉及的具体交换环中,我们都能证明极大理想之存在性,而不必依赖下面将介绍的 Zorn 引理. 因而下面内容是可以略去的. 另一方面讨论极大理想的存在性又是一个学习 Zorn 引理的极好机会,这个引理常被使用,属于集合论基础的公理. 所以我们还是写在这里,留给感兴趣的读者.

设A是一个有 1 的(不一定是交换的)环. 我们用下面的讨论来说明A中必有极大理想. 显然理想I是真理想,当且仅当$1\notin I$. 这样(0)是真理想,若(0)不是极大理想,则必有真理想I_1满足$(0)\subsetneq I_1\subsetneq A$. 对理想$I_1$问同样的问题,这样就得到一串真理想$(0)\subsetneq I_1\subsetneq I_2\subsetneq I_3\subsetneq\cdots$. 在过程中,如果某一$I_n$是极大理想,即我们就证完了,不然就得一个无限串. 令$J=\bigcup_{n=1}^{\infty}I_n$. 容易证明$J$是一个理想. 这是因为若$x,y\in J$,则$x\in I_s,y\in I_t$,此时便有$x,y$都在$I_n$中,$n=\max(s,t)$,但$I_n$是理想,因而$\forall\ a\in A$,$x+y,x-y,ax$,$xa$也都在$I_n$,随之也都在$J$中,这就证明了$J$是一个理想. 由于 1 不属于任意$I_n$,因而 1 也不会属于这些$I_n$的并集$J$中,即$1\notin J$,这就是说$J$仍是一个真理想. 如果$J$仍不是极大理想,就仿上继续作下去而又得到一串真理想$J\subsetneq J_1\subsetneq J_2\subsetneq J_3\subsetneq\cdots$,如果在此过程中,$J_n$仍都不是极大理想,就又得一个递增的无限理想串. 令$K=\bigcup_{n=0}^{\infty}J_n$. 再从真理想$K$开始干同样的事. A是一个固定集合,而另一方面,借助于单位元的存在,我们永远可从一个真理想扩大到另一个较大的真理想上去,我们就应该会在某一步得到一个极大理想.

这个似乎合情合理的说明中似乎有一点没有说透.如果从反面问一下:在上述过程中假设在任何一步都得不到极大理想,会引出什么矛盾来吗?

数学上在遇到这种情况时使用的办法就是:第一把情况说清楚,第二把它作为公理承认下来.Zorn 引理就是针对上述情形的一个公理.

为了把情况说清楚,要引入一些概念,它们在数学中是重要的,常出现的.

定义 4.11 设非空集 M 中有一个二元关系 $\leqslant$. 如果这个关系 $\leqslant$ 满足下列条件:

P1) 自反律: $\forall\ a \in M, a \leqslant a$;

P2) 对称律:若 $a \leqslant b, b \leqslant a$, 则 $a = b$;

P3) 传递律:若 $a \leqslant b, b \leqslant c$, 则 $a \leqslant c$.

则称关系 $\leqslant$ 为 M 的一个偏序,称 $(M, \leqslant)$ 为一个偏序集.

记 $a \leqslant b$ 且 $a \neq b$ 为 $a < b$.

定义 4.12 若 $(M, \leqslant)$ 是一个偏序集,且对任二 $a, b \in M$ 或有 $a \leqslant b$, 或有 $b \leqslant a$, 则称 $(M, \leqslant)$ 为有序集.

设 T 是偏序集 M 的一个子集,称 M 的一个元素 a 为 T 的上界,如果 $\forall\ x \in T, x \leqslant a$. 称偏序集 $(M, \leqslant)$ 的一个子集 T 是有序集(或链),若 $(T, \leqslant)$ 是一个有序集.称偏序集 M 的一个元素 a 为 M 的极大元,如果不存在 $x \in M, a < x$.

Zorn **引理** 一个偏序集 M, 如果它的任意链都有上界,则对 M 中任一元 x, 必有 M 中极大元 m_x 满足关系: $x \leqslant m_x$.

把 Zorn 引理作为公理承认下来,而去证明下面

定理 4.13 设 A 是有 1 的环,则 A 必有极大理想.

证明 令 $M = \{A$ 的所有真理想$\}$. 易见 $(M, \subseteq)$ 是一个偏序集, 其中 $\subseteq$ 是理想之间的包含关系.在 M 中任取一个链 $T = \{I_\lambda, \lambda \in \Sigma\}$, 而往证 T 必有上界.令 $I = \bigcup_{\lambda \in \Sigma} I_\lambda$. 首先 I 是一个理想:任取 $x, y \in I$, 则由于 I 是 I_λ, $\lambda \in \Sigma$, 的并集,故必有 $\lambda, \mu \in \Sigma$, 使得 $x \in I_\lambda$ 而 $y \in I_\mu$. 由于 T 是链,故 I_λ, I_μ 之间有包含关系,不妨设 $I_\lambda \subseteq I_\mu$. 这样 x, y 都在 I_μ 中,对 $\forall\ a \in A, x + y, x - y, ax, xa$ 都在 I_μ 中,随之都在 I 中.这就是证明了 I 是理想.其次,和前面完全一样,由于 I_λ 是真理想,1 不属于每一 I_λ, 随之也不属于它们的并集 I, 这说明 $I \neq A$. 合在一起便说明 I 是真理想,因而 $I \in M$. 显然 $\forall \lambda \in \Sigma$, $I_\lambda \subseteq I$, 故 I 是 T 的一个上界.

这样 A 的真理想组成的偏序集 $(M, \subseteq)$ 满足 Zorn 引理的前提,因而根据 Zorn 引理知, M 有极大元,亦即环 A 有极大理想,并且根据 Zorn 引理还知,任一真理想都可扩大成一个极大理想.□

下面来讨论域 F 上向量空间 V 的基的存在问题.对于有限生成的向量空

间 V，我们在线性代数中已经知道，V 是有(有限)基的. 但对于任意向量空间 V，它是否也有基呢！这是一个较极大理想的存在更使人感兴趣的问题，因为前面已经看到，如果 V 有基，V 中任一元素通过基有一个唯一表达式，这对于我们讨论向量空间的各种性质是非常方便的.

如果向量空间 V 中存在一个极大的线性无关集 B，则 B 就是 V 的一个基. 这里"极大"的意义当然指若 $B \not\subseteq C$，则集 C 就不是线性无关集. 为此只需证明，V 中不在 B 中的任一元素都可表成 B 中有限个元素的线性和. 取 $x \notin B$，令 $C = B \cup \{x\}$.　$B \not\subseteq C$，故 C 不是线性无关的，这就是说在 C 中有一线性相关的有限子集 E. 由于线性无关集 B 的任一有限子集，依定义，都是线性无关的，故必有 $x \in E$，记 $E = \{x, b_1, \cdots, b_n\}$，其中 $b_i \in B$. 此时便有 E 是线性相关的，而 $\{b_1, \cdots, b_n\}$ 是线性无关的，即得 x 可表示成 $b_1, \cdots, b_n$ 的线性和. 这就证明了：极大线性无关集 B 是 V 的基.

这样，证明向量空间 V 的基的存在性就归结为 V 的极大线性无关集的存在性. 有了 Zorn 引理，有了上面证明极大理想存在的经验，证明 V 的极大无关集的存在就没有什么困难了.

设 V 是域 F 上向量空间. 令 M 是 V 中一切线性无关集组成的集合. $(M, \subseteq)$，其中 $\subseteq$ 是集合的包含关系，是一个偏序集. 请读者证明一下，这个偏序集 M 中的每一个链在 M 中都有上界，这样根据 Zorn 引理便得 M 中有极大元 B. 再注意到上面刚证过的事实便得下面

定理 4.14　设 V 是域 F 上向量空间，则 V 有基，且 V 的任一线性无关子集都可扩大成 V 的一个基.

一般言，对于有限的情况，极大元的存在是显然的. 而对于无限的情况，往往利用 Zorn 引理可证得极大元的存在.

练习

1. 设整环 R 的特征为素数 p，证明：

   1) 对任意 $a, b \in R$，有 $(a+b)^{p^n} = a^{p^n} + b^{p^n}$；

   2) $\phi: R \longrightarrow R, a \longmapsto a^p$ 是环同态，称为 Frobenius 同态；

   3) 当 R 是域时，ϕ 是域同构，称为 Frobenius 同构.

2. 设 $\mathbf{Z}[i] = \{a + bi \mid a, b \in \mathbf{Z}\}$. 求证：$\mathbf{Z}[i]/(1+i)$ 是域.

3. 证明：(4) 是偶数环 R 的最大理想，但 $R/(4)$ 不是域.

4. 在 $\mathbf{Z}[i]$ 中的理想 (5) 和 (11) 是不是素理想？

5. 设 $P_1 \supseteq P_2 \supseteq \cdots$ 是交换环 R 的一个素理想降链. 证明：$P = \bigcap_{i=1}^{\infty} P_i$ 是 R 的素理想.

§5 整环的整除理论

本节我们继续讨论以 $\mathbb{Z}$、二次数环、多项式为其特例的整环 R. 主题是把 $\mathbb{Z}$、$F[x]$ 中的整除理论推广到一般的整环上去,而在这一推广过程中引入 Euclid 整环、主理想整环以及唯一分解整环.

分析出并抓住一些重要特例的本质性质,并把它们推广到一般的情形,从而使在具体情形行之有效的工具也能在一般场合发挥作用,这是数学中常用的手法.有的推广很难,有的推广则是有点照猫画虎.本节中的推广是后者,因而也是初学者学习推广工作的一个好机会.

首先回忆一下 $\mathbb{Z}$ 和 $F[x]$ 的整除理论.

在整数环 $\mathbb{Z}$ 中给两个整数(可以为 0) a,b,说 a 整除 b,记作 $a|b$,当且仅当 $b=ac,c\in\mathbb{Z}$. 当 $a|b$ 时,称 a 为 b 的因数,称 b 为 a 的倍数.整除理论的中心问题就是给定 a,b 后,去判断是否有 $a|b$.

在 $\mathbb{Z}$ 中单位元 1 的因数只有 ±1,它们是任何整数的因数,因而在整除理论中心问题中它们是丝毫不起作用的.但常引出一些叙述上的麻烦.

在 $\mathbb{Z}$ 中,若 $a|b$ 且 $b|a$,则称 a,b 为相伴数.整数 a,b 是相伴数当且仅当 $a=\pm b$. 整数 a 永远有 $\pm1,\pm a$ 为它的因数,称它们为 a 的平凡因数.称 a 为素数,如果 $a\neq\pm1$ 且 a 没有非平凡因数.

另外我们还熟知 a,b 的公倍数、最小公倍数、公因数、最大公因数的概念以及 a,b 互素的概念.

我们有整数的绝对值 $|a|$ 的概念,$|a|\in\mathbb{Z}^+\cup\{0\}$. 与绝对值相联系的在 $\mathbb{Z}$ 中有 Euclid 带余除法:任给整数 $a,b\neq0$,则有唯一存在的整数 q 和 r 满足

$$a=bq+r,\quad 0\leqslant r<|b|.$$

熟知地,由 Euclid 算法我们可证得:

Z1) 整数 a,b 的最大公因数 $(a,b)=as+bt,s,t\in\mathbb{Z}$.

Z2) 若 p 是素数且 $p|ab$,则必有 $p|a$ 或 $p|b$.

Z3) 算术基本定理

(1) 任一非零非 ±1 的整数 $a=p_1p_2\cdots p_n$,所有 p_i 都是素数(分解的存在性);

(2) 若 $a=p_1p_2\cdots p_n=q_1q_2\cdots q_m$,所有 p_i,q_i 都是素数,则必有 $n=m$,且适当排列后可得对任意 i,有 $p_i=\pm q_i$(分解的唯一性).

如果再回忆一下证明的细节，我们会发现，由整数绝对值的性质（即 a 是 b 的真因数，则 $|a|<|b|$）便有整数分解的存在性，而 Euclid 算法 ⇒ Z1) ⇒ Z2) ⇒ 整数分解的唯一性.

对于数域 F 上的一元多项式环 $F[x]$，我们类似地也有整除、相伴多项式、因式、真因式、不可约多项式、最大公因式、最小公倍式等概念，就不在这里重提它们的定义了. 要注意的是，$F[x]$ 中的单位元 1 的因子是数域 F 中所有非零的数，因而两个多项式 $f(x),g(x)$ 是相伴的当且仅当 $f(x)=a\cdot g(x), 0\neq a\in F$. 这就是说，在整除理论中 $\mathbb{Z}$ 中的 ± 1 和 $F[x]$ 中的非零常数是处在彼此相应的位置上.

我们有非零多项式 $f(x)$ 的次数 $\deg f$ 的概念，$\deg f\in\mathbb{Z}^+\cup\{0\}$. 与 $\deg f$ 相联系的在 $F[x]$ 中也有 Euclid 带余除法：任给 $F[x]$ 中多项式，$f(x), g(x)\neq 0$，则有唯一存在的多项式 $q(x)$ 和 $r(x)$ 满足：

$$f(x)=g(x)q(x)+r(x),\quad \deg r<\deg g \text{ 或 } r=0.$$

熟知地，和数环 $\mathbb{Z}$ 中的证明完全平行地，由 $F[x]$ 中的 Euclid 算法我们可证得：

F1) 多项式 $f(x),g(x)$ 的最大公因式 $(f(x),g(x))=f(x)s(x)+g(x)t(x)$，$s(x),t(x)\in F[x]$.

F2) 若 $p(x)$ 是不可约多项式，且 $p(x)\mid f(x)g(x)$，则必有 $p(x)\mid f(x)$ 或 $p(x)\mid g(x)$.

F3) 唯一分解定理

(1) 任一非常数一元多项式 $f(x)=p_1(x)p_2(x)\cdots p_n(x)$，所有 $p_i(x)$ 都是不可约多项式（分解的存在性）；

(2) 若 $f(x)=p_1(x)p_2(x)\cdots p_n(x)=q_1(x)q_2(x)\cdots q_m(x)$，所有 $p_i(x),q_j(x)$ 都是不可约多项式，则必有 $n=m$，且适当排列后可得对任意 i，存在 $a_i\in F$，使得 $p_i=a_iq_i$（分解的唯一性）.

同样，回想一下相应的证明，你会发现，由一元多项式 $f(x)$ 的次数 $\deg f(x)$ 的性质（即 $f(x)$ 是 $g(x)$ 的真因式，则 $\deg f(x)<\deg g(x)$）便得 $f(x)$ 的分解的存在性，而 Euclid 算法 ⇒ F1) ⇒ F2) ⇒ $f(x)$ 分解的唯一性.

关于 $\mathbb{Z}, F[x]$ 我们有下面

命题 5.1 1) 整数环 $\mathbb{Z}$ 中任意理想都是主理想.

2) 数域 F 上一元多项式环 $F[x]$ 中任意理想都是主理想.

证明 1) 设 I 是 $\mathbb{Z}$ 的非零理想，则 $N=\{|a|, 0\neq a\in I\}$ 是 $\mathbb{Z}^+$ 的非空子集，命其中最小数为 n 而取 $a\in I, |a|=n$. 今证 $I=(a)$. 任取 $b\in I$，由 Euclid 算法得 $b=qa+r$，其中 $r=0$ 或 $0<r<|a|$. 由于 $r=b-qa$

$\in I$，故后一种情形由于 a 的选择不可能发生，即必 $r=0$，亦即 $b=qa\in(a)$. 这就证得 $I=(a)$.

2) 设 I 是 $F[x]$ 的非零理想，则 $N=\{\deg f(x), 0\neq f(x)\in I\}$ 是 $\mathbb{Z}^+\cup\{0\}$ 的非空子集，命其中最小数为 n 而取 $f(x)\in I, \deg f(x)=n$. 利用 $F[x]$ 的 Euclid 算法容易证明：$I=(f(x))$. □

我们详细地复习了 $\mathbb{Z}$ 和 $F[x]$ 的整除理论之后，把它推广到一般环上去该不是很困难的事了，至少是有路可循了. 对非交换环，或者有零因子的环，对它们讨论整除理论，因为太泛而不会有好的结果的. 自然地要限制在整环而非域的范围内，因为对于域而言，每个非零元是任意元的因子，因而无整除理论好谈.

设 R 是整环，我们首先把 R 的整除理论的基本概念介绍一下.

设 $a,b\in R$，a 整除 b，记作 $a|b$，当且仅当 $b=ac, c\in R$. 当 $a|b$ 时，称 a 是 b 的因子，b 是 a 的倍元. 称单位元 1 的因子为 R 的单位. 称 a,b 为相伴元，如果 $a=\alpha b$，α 是单位. 非零元 a 永远有单位及其相伴元为其因子，这些称为 a 的平凡因子. 没有非平凡因子的非零元称为 R 的既约元.

我们有理想特别是主理想的概念，主理想 $(a)=\{ar, r\in R\}$ 刚好就是 a 的一切倍元的集合. 因而用主理想的语言去表达上述基本概念是很方便的：

a 整除 $b\Longleftrightarrow b\in(a)$；

α 是 R 的单位 $\Longleftrightarrow(\alpha)=R$；

a,b 为相伴元 $\Longleftrightarrow(a)=(b)$；

b 是 a 的真因子 $\Longleftrightarrow (a)\subsetneq(b)\subsetneq R$；

a 是既约元 $\Longleftrightarrow(a)$ 是极大主理想.

在前面的回顾中，我们特别注意到性质 Z2)和 F2)对分解的唯一性是至关重要的.

定义 5.2 整环 R 中元素 p 称作素元，如果对任意 $a,b\in R$，有 $p|ab$ 则必有 $p|a$ 或 $p|b$.

命题 5.3 在整环 R 中，p 是素元当且仅当 (p) 是素理想.

证明 (p) 是素理想 $\Longleftrightarrow ab\in(p)$ 必 $a\in(p)$ 或 $b\in(p)$. 把一个元素属于一个主理想的事实用整除的语言去叙述，后者就是：$p|ab$ 则必 $p|a$ 或 $p|b$. □

在上节中我们知道极大理想是素理想，但极大主理想(所有主理想中的极大元)和极大理想(所有理想中的极大元)尚有一定距离. 故在一般整环中既约元和素元是两个不同的概念.

命题 5.4　1) 在整环 R 中，素元必是既约元.

2) 在整环 R 中，若每一既约元都是素元，则在 R 中元素分解的唯一性成立，即若 $a = p_1p_2\cdots p_s = q_1q_2\cdots q_t$，$p_i$ 和 q_j 是既约元，则必有 $s = t$，而适当编序后有 p_i 和 q_i 是相伴元.

证明　1) 由素元和既约元的定义可得.

2) 和 $\mathbb{Z}$ 中整数分解的唯一性证明是一样的. □

我们知道，在 $\mathbb{Z}$ 和 $F[x]$ 中有了唯一分解定理，关于整除的一些基本问题，诸如判断一个元素是否整除另一个元素，求两个元素的最大公因式，最小公倍式，都可以从这些元素的唯一分解式直接读出来. 因而找出一些充分条件以保证一个整环是下面定义的唯一分解环是我们感兴趣的一个问题.

定义 5.5　一个整环 R 称作是唯一分解环，如果

D1) R 中任一非零非单位元 $a = p_1p_2\cdots p_n$，所有 p_i 都是既约元(分解的存在性)；

D2) 若 $a = p_1p_2\cdots p_n = q_1q_2\cdots q_m$，所有 p_i, q_i 都是既约元，则必有 $n = m$，且适当排列后可得对任意 i，有 $(p_i) = (q_i)$ (分解的唯一性).

一个摆在我们面前这样的充分条件就是 Euclid 算法. 为此需要把 $\mathbb{Z}$ 和 $F[x]$ 都有的 Euclid 算法统一起来，用一般整环的语言表述出来就行了.

定义 5.6　1) 称一个整环 R 有 Euclid 除式，如果

(a)有一映射

$$\phi: \{R \text{ 的非零元全体}\} \longrightarrow \mathbb{Z}^+ \cup \{0\};$$

(b)任给 R 中元素 $a, b \neq 0$，则有 q, r 满足

$$a = bq + r, \text{其中 } r = 0 \quad \text{或} \quad \phi(r) < \phi(b). \tag{1}$$

2) 称有 Euclid 除式的整环 R 为 Euclid 环.

当然在 Euclid 环中，给了 a 和 $b \neq 0$，并没有一个算法可算出满足(1)的 q, r，这和在 $\mathbb{Z}$ 和 $F[x]$ 中有一个 Euclid 算法是不一样的. 在 Euclid 环中我们并没有要求满足(1)的 q, r 的唯一性，原因是(1)的存在性足以保证 Euclid 环是一个唯一分解环. 这就是

定理 5.7　Euclid 环是唯一分解环. □

运用 $\mathbb{Z}$ 和 $F[x]$ 中唯一分解定理的证明思路，严格用整环中的语言把它们表述出来，我们就很容易证明上面这个定理. 我们把这工作留给读者. 当然从下面的讨论中，作为推论也将得到这个定理.

定义 5.8　若一个整环的每个理想都是主理想(即由一个元素生成的理想)，就称之为主理想整环.

命题 5.9　Euclid 环是主理想整环. □

证明留给读者.

下面证明主理想整环 R 必是唯一分解环.

先考察分解的存在性.任取 $0 \neq a \in R$,a 不是单位,而问 a 是否为既约元.若是,则已得 a 的分解,若否,则 $a = a_1 b_1$,这里 a_1, b_1 是 a 的非平凡因子.再对 a_1, b_1 问同样的问题,如此继续下去.什么时候 a 没有分解式呢?那就是 a 有非平凡因子 c_1,c_1 有非平凡因子 $c_2, \cdots, c_n$ 有非平凡因子 $c_{n+1}, \cdots$,并且是无限地分解下去.这种情况,用理想的语言来表述,就是存在无限严格递升主理想链:

$$(a) \subsetneq (c_1) \subsetneq (c_2) \subsetneq \cdots \subsetneq (c_n) \subsetneq \cdots \tag{2}$$

排除这种情况的办法就是要求下面条件成立

定义 5.10 称一个环 R 对主理想满足极大条件,如果 R 中任一无限递升主理想链

$$(c_1) \subsetneq (c_2) \subsetneq \cdots \subsetneq (c_n) \subsetneq \cdots \tag{3}$$

在有限步必停下来,即存在 N,使得 $(c_N) = (c_{N+i}), i \in \mathbb{Z}^+$.

命题 5.11 1) 主理想整环 R 对主理想满足极大条件.

2) 在主理想整环 R 中每一非单位,非零元素都可表成一些既约元的乘积(分解的存在性).

证明 1) 在 R 中任取一无限递升主理想链(3).令 $I = \bigcup_i (c_i)$.我们知道 I 是一个理想.但依定义,在主理想环 R 中,每一理想都是主理想,故 $I = (b), b \in R$.由 $b \in I$ 而 I 是 (c_i) 的并集,故必存在一 N 使 $b \in (c_N)$.这样 $(b) \subseteq (c_N) \subseteq I = (b)$,从而 $(c_N) = (c_{N+i}), i \in \mathbb{Z}^+$,即 R 对主理想满足极大条件.

2) 任取非单位非零元 $a \in R$.若 a 是既约元,则得 a 的分解式,不然 $a = a_1 b_1$,这里 a_1, b_1 是 a 的真因子,再对 a_1, b_1 问同样的问题,如此继续下去.此时或者在有限步内 a 分解成一些既约元乘积,或者得到一无限严格递升主理想链(2).由 1)知后者不可能出现,因而得到 a 的分解的存在性.□

其次来考察分解的唯一性.过去关于 $\mathbb{Z}$ 和 $F[x]$ 的讨论中,我们都熟悉:命题 Z1)(F1)) ⇒ 命题 Z2)(F2)) ⇒ 分解的唯一性的推导过程.就是说,如果对一个整环我们能有类似 Z1)和 F1)的命题,那就驾轻就熟地可以由之得到类似 Z2)和 F2)的命题,以及分解的唯一性.下面就来做这件事.

在一个整环 R 中,称元素 d 是 a, b 的公因子,如果 $d \mid a, d \mid b$.称 a, b 的一个公因子 d 为极大公因子,如果对 a, b 的任意公因子 c 都有 $c \mid d$.易见 a, b 的极大公因子不是唯一的,但它们必是相伴的.在这种意义下,我们用 (a, b) 表示 a, b 的极大公因子.若 $(a, b) = 1$ (或单位),则称 a, b 互素.

根据理想的定义,可直接验证下面

引理 5.12　在一个环中,两个理想 I,J 之和 $I+J=\{x+y,x\in I,y\in J\}$ 仍是 R 的理想.特别,主理想 $(a),(b)$ 之和 $(a)+(b)=\{ax+by|x,y\in R\}$ 是理想,但一般不一定是主理想.□

命题 5.13　在主理想整环 R 中,(a,b) 可表成 a,b 的线性和,即存在 $s,t\in R$ 使得 $(a,b)=sa+tb$.

证明　主理想 $(a),(b)$ 之和 $(a)+(b)$ 是 R 的一个理想,但 R 是主理想环,故有 $d\in R$ 使得 $(a)+(b)=(d)$,因而存在 $s,t\in R$,使得 $d=sa+tb$.由于 $a\in(d),b\in(d)$ 故 $d|a,d|b$,即 d 是 a,b 的一个公因子.但另一方面,$d=sa+tb$,由之显然有 a,b 的公因子 c 必是 d 的因子,即得 d 就是 a,b 的一个极大公因子.□

由这个命题读者可以容易地得下面两命题.

命题 5.14　在主理想整环 R 中,既约元都是素元.□

命题 5.15　在主理想整环 R 中,元素分解的唯一性成立.□

命题 5.11 和上命题合在一起便是

定理 5.16　主理想整环是唯一分解环.□

这样我们有 Euclid 环类 $\subseteq$ 主理想整环类 $\subseteq$ 唯一分解环类.下面将会看到这里的包含关系是真包含关系.

在完成 $\mathbb{Z}$ 和 $F[x]$ 的整除理论之后,接着很自然地是对下列诸具体整环讨论整除问题:与整数环 $\mathbb{Z}$ 最接近的二次实数环 $\mathbb{Z}[\sqrt{d}]=\{a+b\sqrt{d}|a,b\in\mathbb{Z}\}$,二次复数环 $\mathbb{Z}[\sqrt{-d}]=\{a+b\sqrt{-d}|a,b\in\mathbb{Z}\}$,这里 d 为无平方因数的正整数;域 F 上一元多项式 $F[x]$ 的推广 $F[x_1,\cdots,x_n]$,以及 $\mathbb{Z}$ 上一元多项式环 $\mathbb{Z}[x]$.现在就来逐一讨论.

设 d 是无平方因数的正整数,而来讨论复二次数环 $\mathbb{Z}[\sqrt{-d}]$ 的整除理论.为方便计,把 $\sqrt{-d}$ 记作 α.

易知 $\mathbb{Z}[\alpha]$ 的分式域是复二次数域 $\mathbb{Q}[\alpha]=\{a+b\sqrt{-d},a,b\in\mathbb{Q}\}$.对 $x\in\mathbb{Q}[\alpha]$ 用 $\bar{x}$ 表复数 x 的共轭数,规定 $x=a+b\alpha$ 范数

$$N(x)=x\bar{x}=a^2-b^2\alpha^2=a^2+b^2d.$$

易知 $\forall\ x,y\in\mathbb{Q}[\alpha],N(xy)=N(x)N(y)$.

而当 $0\neq x\in\mathbb{Z}[\alpha]$ 时,$N(x)$ 是正整数.容易证明下面

命题 5.17　设 d 是无平方因数的正整数,在复二次数环 $\mathbb{Z}[\sqrt{-d}]$ 中有

1) 对任意正整数 n,$N(x)=n$ 的 x 只有有限多个.

2) x 是单位当且仅当 $N(x)=1$,随之只有有限个单位.

3) 与 x 相伴的元素只有有限多个.

4) 任取 $0\neq x\in\mathbb{Z}[\sqrt{-d}]$,则 x 的因子只有有限多个.

5) $\mathbb{Z}[\sqrt{-d}]$ 中任意非零,非单位元都可分解成既约元的乘积.□

C.F.Gauss(1777－1855)第一个深入地研究了 $\mathbb{Z}[i]$. 这开始了现在称之为代数数论的研究,后人称 $\mathbb{Z}[i]$ 为 Gauss 环.

命题 5.18 Gauss 环 $\mathbb{Z}[i]$ 是 Euclid 环,因而是唯一分解环.

证明 我们的范数 $N(x)$ 给出 $\mathbb{Z}[i]$ 到 $\mathbb{Z}^+\cup\{0\}$ 的一个函数. 今证 $\mathbb{Z}[i]$ 有 Euclid 除式. 任取 $\alpha, 0\neq\beta\in\mathbb{Z}[i]$, 要证必有 $\delta,\gamma\in\mathbb{Z}[i]$ 使得 $\alpha=\beta\delta+\gamma$ 且 $N(\gamma)<N(\beta)$ 或 $\gamma=0$ (即 $N(\gamma)=0$). 在域 $\mathbb{Q}[i]$ 中用 $0\neq\beta$ 去除 $\alpha=\beta\delta+\gamma$ 的两侧,便得 $\frac{\alpha}{\beta}=\delta+\frac{\gamma}{\beta}$, 而上面要求的条件 $N(\gamma)<N(\beta)$ 就变成 $N(\frac{\gamma}{\beta})<1$. 因而命题的证明就归结为:给定 $\frac{\alpha}{\beta}=a+bi\in\mathbb{Q}[i]$, 必有 $\delta=s+ti\in\mathbb{Z}[i]$ 使 $N(\frac{\alpha}{\beta}-\delta)<1$, 这样只要取离有理数 a 最近的整数 s 和离 b 最近的整数 t, 使得 $|a-s|\leqslant\frac{1}{2}, |b-t|\leqslant\frac{1}{2}$, 这时就有

$$N(\frac{\alpha}{\beta}-\delta)=N((a-s)+(b-t)i)$$

$$=(a-s)^2+(b-t)^2\leqslant\frac{1}{2}<1.$$

这就证明 $\mathbb{Z}[i]$ 是 Euclid 环. □

下面例子说明,有许多复二次数环 $\mathbb{Z}[\sqrt{-d}]$ 不是唯一分解环.

例 在 $\mathbb{Z}[\sqrt{-5}]$ 中,数 6 有下面两个分解

$$6=1-(-5)=(1+\sqrt{-5})(1-\sqrt{-5}),\quad 6=2\cdot 3.$$

利用范数,不难得到 $\mathbb{Z}[\sqrt{-5}]$ 中的单位 $\alpha=a+b\sqrt{-5}$ 满足

$$N(\alpha)=N(a+b\sqrt{-5})=a^2+b^2 5=1,$$

故只有两个单位 ±1. 而 $N(2)=4, N(3)=9, N(1+\sqrt{-5})=6=N(1-\sqrt{-5})$. 且 $\mathbb{Z}[\sqrt{-5}]$ 中不存在数 α, 使 $N(\alpha)=2$ 或 $N(\alpha)=3$, 故知 $2,3,1+\sqrt{-5},1-\sqrt{-5}$ 都是既约元,且这四个数间并没有相伴关系. 这就说明 $\mathbb{Z}[\sqrt{-5}]$ 是一个分解存在,但分解不唯一的整环.

类似地,在 $\mathbb{Z}[\sqrt{-13}]$ 中我们有

$$14=1+13=(1+\sqrt{-13})(1-\sqrt{-13})=2\cdot 7,$$

即 14 有两种本质上不同的既约元的分解. 作为练习当 $-d=4n+3, n\geqslant 2$ 时考虑 $1+d$ 的分解,可以证明 $\mathbb{Z}[\sqrt{-d}]$ 是一个分解存在而不唯一的整环.

下面介绍一下关于二次代数整数环的结果而略去证明. $\mathbb{C}$ 中数 θ 称为 $\mathbb{Q}$ 上代数数,如果它是 $\mathbb{Q}$ 上某个多项式 $f(x)$ 的根. θ 称为 n 次代数数,如果 $\deg f(x)$ 为 n. θ 称为代数整数,如果它是 $\mathbb{Z}$ 上某个最高次数项的系数为 1

的多项式的根. 容易证明二次代数数域(即含一个二次代数数 θ 的最小数域)可表成 $\mathbb{Q}[\sqrt{m}]$, 其中 m 是无平方因数的整数. $\mathbb{Q}[\sqrt{m}]$ 中所有代数整数的集合,用符号 $I(\sqrt{m})$ 记之,可以证明它是一个数环,称之为二次代数整数环. 可以证明:

当 $m \equiv 2,3 \pmod 4$ 时, $I(\sqrt{m}) = \mathbb{Z}[\sqrt{m}]$.

当 $m \equiv 1 \pmod 4$ 时, $I(\sqrt{m}) = \mathbb{Z}[-1/2 + \sqrt{m}/2]$.

例如 $I(\sqrt{-1}) = \mathbb{Z}[i], I(\sqrt{19}) = \mathbb{Z}[\sqrt{19}]$, $I(\sqrt{-3}) = \mathbb{Z}[-1/2 + \sqrt{-3}/2]$ 等等.

关于复二次代数整数环 $I(\sqrt{-d}), d > 0$, 我们有很漂亮的结果: $I(\sqrt{-d})$ 是唯一分解整环当且仅当 $-d = -1, -2, -3, -7, -11, -19, -43, -67, -163$. 其中"当"部分是 Gauss 在约 190 年前证明的,他并猜测"仅当"部分也该成立,但"仅当"部分直到 1966 年才被 Baker 和 Stark 证出. 另外我们还知道. 只有当 $-d = -1, -2, -3, -7, -11$ 时 $I(\sqrt{-d})$ 是 Euclid 环.

关于实二次代数整数环 $I(\sqrt{d}), d > 0$, 只就 $I(\sqrt{d}) = \mathbb{Z}[\sqrt{d}]$ 的情况简单提一下. 很自然的,对 $\alpha = a + b\sqrt{d}, a, b \in \mathbb{Z}$, 引进共轭数 $\bar{\alpha} = a - b\sqrt{d}$ 而考虑乘积 $N(\alpha) = \alpha\bar{\alpha} = a^2 - b^2 d$. 由于 d 是正整数, $\alpha\bar{\alpha}$ 可能取负值(这和复二次数环中 $\alpha\bar{\alpha}$ 永远是非负的情况,很不一样),这样我们只好考虑 α 的范数 $N(\alpha)$ 的绝对值 $|N(\alpha)|$, 它是定义域为 $\mathbb{Z}[\sqrt{d}]$ 而取值在 $\mathbb{Z}^+ \cup \{0\}$ 中的一个函数,因而符合 Euclid 算法中对所用函数的基本要求. 当然这里也有 $N(\alpha\beta) = N(\alpha)N(\beta)$. 容易证明: α 是单位当且仅当 $|N(\alpha)| = 1$. 由之,若 α 是既约元,则 $|N(\alpha)| \geqslant 2$, 这样,任一元素 β 最多可分成 $|N(\beta)|/2$ 个既约元的乘积,故知在 $\mathbb{Z}[\sqrt{d}]$ 中元素的分解是存在的.

为了感觉一下这里的困难和特点,看一下 $I(\sqrt{2}) = \mathbb{Z}[\sqrt{2}]$ 的单位,易见 $\alpha = a + b\sqrt{2}$ 是单位当且仅当 $|N(\alpha)| = 1$, 即 $|a^2 - b^2 2| = 1$. 由之知 $\omega = 1 + \sqrt{2}$, 随之 ω^n 都是单位,即有无穷多个单位;另外可以想象,范数为某一正整数 n 的彼此不相伴的因子也可能有无穷多个,而这的确是可以证明的. 虽然如此,Gauss 猜想:有无穷多个实二次代数整数环是唯一分解环. 这一猜想至今仍没有解决. 另一方面,我们知道实二次代数整数环 $I(\sqrt{d})$ 是 Euclid 环当且仅当 $d = 2,3,5,6,7,11,13,17,19,21,29,33,37,41,57,73$.

这里有一段史话. 由于理想和环的同态联系得那样自然和紧密,常会觉得理想是和同态同时出现的. 殊不知理想的最初出现是和代数整数环元素的唯一分解问题相伴的. 从上面二次代数整数环的讨论已经看到元素的分解常不是唯一的. 元素相当于主理想,元素的分解相当于把主理想表示成一些素主理想的乘积. 既然有时这样的分解常不唯一,为什么不可以用研究理想(不管它是不是主理想)的分解成素理想的乘积来代替元素的分解? 在这个更广阔的

背景下，也许能有分解的唯一性. 在数系扩张的过程中，我们曾看到过，在一个宽松的场合中，某些问题常能得到一个满意的解决. E. E. Kummer(1810－1893)就是这样作的，他第一个在代数整数环中引入"理想数"(就是现在的理想)的概念. 关于理想(数)的分解这里不再进一步讨论，只是叙说一下，对代数整数环(例如上面的二次整数环)的理想有唯一分解定理.

现在来讨论多项式环，即 $\mathbb{Z}[x]$ 以及域 F 上多项式环 $F[x_1,\cdots,x_n]$ 的唯一分解问题. 由于 $F[x_1,x_2]=F[x_1][x_2]$，故可归结为：假设 R 是唯一分解环，问 $R[x]$ 是否仍为唯一分解环. 当然也可以问：若 R 是 Euclid 环或主理想整环，$R[x]$ 是否也是. 但从 $\mathbb{Z}[x]$ 不是主理想环，可知后面问题不会有肯定结果.

下面证明：$\mathbb{Z}[x]$ 是唯一分解环.

取 $\mathbb{Z}$ 的分式域 $\mathbb{Q}$，　$\mathbb{Z}[x]$ 当然是 $\mathbb{Q}[x]$ 的一个子环. $\mathbb{Q}[x]$ 是唯一分解环. 因而证明的关键在于：$\mathbb{Z}[x]$ 中非常数的既约多项式是否仍是 $\mathbb{Q}[x]$ 的既约多项式.

任取 $f(x)\in\mathbb{Z}[x]$. 把 $f(x)$ 的所有系数的最大公因数提出来便得 $f(x)=ag(x)$，其中 $g(x)\in\mathbb{Z}[x]$，而其所有系数的最大公因数为 1，这个概念很有用，写成

定义 5.19　$g(x)\in\mathbb{Z}[x]$. 若 $g(x)$ 的所有系数的最大公因数为 1，就称 $g(x)$ 为本原多项式.

$\mathbb{Z}[x]$ 中的既约元可分两类：常数既约元，这就是 $\mathbb{Z}$ 中的正负素数，还有就是次数 $\geqslant 1$ 的既约多项式 $g(x)$，显然这时 $g(x)$ 必是一个本原多项式.

先讨论分解的存在性. 任取非单位，非零多项式 $f(x)\in\mathbb{Z}[x]$. 由上知 $f(x)=ag(x)$，$a\in\mathbb{Z}$，而 $g(x)$ 是本原多项式. 显然 a 可表为 $\mathbb{Z}[x]$ 中常数既约元的乘积. 另一方面，本原多项式 $g(x)$ 没有常数既约元作为其因子，其因子只能是次数 $\geqslant 1$ 的整系数多项式，利用多项式的次数可知 $g(x)$ 最多可分解 $\deg g(x)$ 个因子的乘积而不会无限制的分解下去. 合起来便得 $f(x)$ 可分解成既约元的乘积.

再讨论分解的唯一性. 这本质上就是要证：$\mathbb{Z}[x]$ 的非常数的本原多项式 $g(x)$，若在 $\mathbb{Z}[x]$ 中是既约元，则在 $\mathbb{Q}[x]$ 中 $g(x)$ 也是既约元. 用反证法，而设 $g(x)$ 在 $\mathbb{Q}[x]$ 中可约，即有 $g(x)=s(x)\cdot t(x)$，$s(x),t(x)\in\mathbb{Q}[x]$，它们的次数 $\geqslant 1$. 对 $s(x),t(x)$ 处理一下，就可得 $s(x)=q\cdot s_0(x)$，$t(x)=r\cdot t_0(x)$，其中 $q,r\in\mathbb{Q}$ 而 $s_0(x),t_0(x)$ 是 $\mathbb{Z}[x]$ 中的本原多项式. 这样

$$a\cdot g(x)=b\cdot s_0(x)\cdot t_0(x),\quad a,b\in\mathbb{Z},a,b\text{ 互素}.$$

由之得 b 整除 $a\cdot g(x)$ 的每一个系数，但 b,a 互素，故 b 整除 $g(x)$ 的每

一系数.但 $g(x)$ 是本原多项式,这样必有 $b=\pm 1$, 如果我们能证:两个本原多项式 $s_0(x),t_0(x)$ 的乘积仍是本原多项式,则重复刚作的讨论可得 $a=\pm 1$. 这样也就得 $g(x)$ 在 $\mathbb{Z}[x]$ 中是可分解的,而和 $g(x)$ 是 $\mathbb{Z}[x]$ 的既约多项式相矛盾.这也就完成了 $g(x)$ 在 $\mathbb{Q}[x]$ 中也是既约元的证明.

Gauss **引理**　设 $s(x),t(x)\in\mathbb{Z}[x]$, 则 $s(x),t(x)$ 是本原多项式当且仅当 $s(x)t(x)$ 是本原多项式.

证明　只需证: $s(x),t(x)$ 是本原多项式,则 $s(x)t(x)$ 也是.介绍两个证法.

证法 1　设 $s(x)=a_0+a_1x+\cdots+a_nx^n, t(x)=b_0+b_1x+\cdots+b_mx^m$. 而

$$s(x)t(x)=c_0+c_1x+\cdots+c_{n+m}x^{n+m}.$$

只需证明对任一素数 p, 必有一系数 $c_k, p\nmid c_k$. 由于 $s(x)(t(x))$ 是本原多项式,必有系数不能被 p 整除.设第一个不被 p 整除的系数为 $a_i(b_j)$, 即 $p|a_l, l<i(p\mid b_k, k<j)$, 且 $p\nmid a_i(p\nmid b_j)$, 此时令 $k=i+j$ 而考察

$$c_k=a_ib_j+a_{i+1}b_{j-1}+\cdots+$$
$$a_kb_0+a_{i-1}b_{j+1}+a_{i-2}b_{j+2}+\cdots+a_0b_k.$$

上式右侧中除 a_ib_j 外其余各项均被 p 整除,但 $p\nmid a_ib_j$, 因而 $p\nmid c_k$. □

证法 2　对任一素数 p, 考虑有限域 $\mathbb{Z}_p=\mathbb{Z}/(p)=\{\overline{n}=n+(p), n\in\mathbb{Z}\}$, 提醒一下: $\overline{n}=\overline{0}$ 当且仅当 $p|n$. 我们知道有同态对应

$$\phi:\mathbb{Z}\longrightarrow\mathbb{Z}_p=\mathbb{Z}/(p)$$
$$n\longmapsto\overline{n}.$$

利用 ϕ 可如下得到一个集 $\mathbb{Z}[x]$ 到集 $\mathbb{Z}_p[x]$ 上的对应,仍记作

$$\phi:\qquad\mathbb{Z}[x]\longrightarrow\mathbb{Z}_p[x]$$
$$a_0+a_1x+\cdots+a_mx^m\longmapsto\overline{a_0}+\overline{a_1}x+\cdots+\overline{a_m}x^m.$$

直接验证可知 ϕ 是环 $\mathbb{Z}[x]$ 到环 $\mathbb{Z}_p[x]$ 上的同态对应.任取 $f(x)\in\mathbb{Z}[x]$, 易知 $\phi(f(x))=0$ 当且仅当 p 整除 $f(x)$ 的每一个系数.

设 $s(x),t(x)$ 是 $\mathbb{Z}[x]$ 中两个本原多项式.此时 $\phi(s(x))\neq 0,\phi(t(x))\neq 0$. 由于 $\mathbb{Z}_p[x]$ 是一个整环,因而没有零因子,所以

$$\phi(s(x)t(x))=\phi(s(x))\cdot\phi(t(x))\neq 0,$$

即多项式 $s(x)t(x)$ 的系数 c_i 有不被 p 整除者.但这里 p 可以是任意素数,即证得所有系数 c_i 的最大公因数为 1,即 $s(x)t(x)$ 是本原多项式.□

比较一下两个证法是有趣的.第一证法突出一个具体技巧,而第二个证法则借用数论中的一个一般技巧:把整数的问题转移到 $\mathbb{Z}_p$ 上去看一看.

有了 Gauss 引理,以及它前面的一些讨论便得

命题 5.20 $g(x)$ 是 $\mathbb{Z}[x]$ 中非常数本原多项式. $g(x)$ 是 $\mathbb{Z}[x]$ 的既约元当且仅当 $g(x)$ 是 $\mathbb{Q}[x]$ 的既约元.

定理 5.21 $\mathbb{Z}[x]$ 是唯一分解环.

证明 上面已证分解的存在性.今证分解的唯一性.

设 $\mathbb{Z}[x]$ 中非零,非单位的多项式 $f(x) = p_1\cdots p_l \cdot s_1(x)\cdots s_n(x) = q_1\cdots q_r \cdot t_1(x)\cdots t_m(x)$, 其中 p_i, q_i 是 $\mathbb{Z}[x]$ 中的常数既约元(即正负素数),而 $s_i(x), t_i(x)$ 是 $\mathbb{Z}[x]$ 中的非常数既约元.令

$$p = p_1\cdots p_l, \quad s(x) = s_1(x)\cdots s_n(x),$$
$$q = q_1\cdots q_r, \quad t(x) = t_1(x)\cdots t_m(x).$$

则有

$$f(x) = p\cdot s(x) = q\cdot t(x).$$

注意到 $s_i(x), t_i(x)$ 是本原多项式,因而依 Gauss 引理, $s(x), t(x)$ 也是本原多项式.易知(类似前面的讨论)整数 p 和 q 必相伴,即 $p = \pm q$, 因而也有 $s(x) = \pm t(x)$.

由 $p = \pm q$ 及 $\mathbb{Z}$ 是唯一分解环知必有 $l = r$, 而重新编号后有 $p_i = \pm q_i$, $i = 1,\cdots,l$. 由 $s(x) = \pm t(x)$ 及 $\mathbb{Q}[x]$ 是唯一分解环,以及命题 5.20 知:必有 $n = m$. 而重新编号后有 $s_i(x) = a_i t_i(x), i = 1,\cdots,n = m$, 其中 a_i 是 $\mathbb{Q}[x]$ 中的单位,即 $a_i \in \mathbb{Q}$. 再用一下上面用过几次的事实,知 $a_i = \pm 1$, 即 $s_i(x) = \pm t_i(x)$, 亦即 $s_i(x)$ 和 $t_i(x)$ 在 $\mathbb{Z}[x]$ 中是相伴元.这样就证明了分解的唯一性.□

掌握上面这个 $\mathbb{Z}[x]$ 的定理的证明思路,就得到下面

定理 5.22 若 R 是唯一分解环,则 $R[x]$ 也是唯一分解环.

推论 5.23 域 F 上多项式环 $F[x_1,\cdots,x_n]$ 是唯一分解环.

至此我们结束关于整环的整除理论的介绍.应该提一下的是:整环的唯一分解定理(算术基本定理)对于整环的整除问题的讨论有点类似复数域的代数基本定理对于多项式根的讨论,只是理论上一个保证,还有很多事要作.例如,二次代数整数环(或者 $\mathbb{Z}[x]$, 或 $F[x_1,\cdots,x_n]$)中既约元是什么样子,给出了一个元素会具体找出分解式吗? 这些常是很难的事情,很多问题都还没有得到解决.

练习

1.在 $\mathbb{Z}[i]$ 中,

1) 求证 $a+bi$ 是单位的充要条件是 $|a+bi|=1$，这里 $|a+bi|$ 是 $a+bi$ 的模．并且求 $\mathbb{Z}[i]$ 的所有单位；

2) 证明：$1-2i$ 是既约元．

2. 证明：$\mathbb{Z}[\sqrt{2}]=\{a+b\sqrt{2}\mid a,b\in\mathbb{Z}\}$ 是 Euclid 环．

3. 证明：Euclid 环是主理想整环．

4. 证明：主理想整环的商环是主理想整环．

5. 证明：在唯一分解整环 R 中，任意两个元素都有一个最大公因子．

6. 设 R 为唯一分解整环，$0\neq a\in R$，则 R 仅有有限个含 a 的主理想．

§6　环的表示与模

我们已熟悉群可分两大类：一是抽象群，即在一个一般集合上，用公理刻画其上的一个运算而得到的；二是具体群，如一个矩阵集关于矩阵的运算作成的群，一个变换集关于变换的乘法作成的群等等．总之在这些群中元素是具体的，运算也是具体的．研究群的方法之一就是把抽象群和具体群联系起来，当然这里联系的方式只有一种，那就是同态，Cayley 定理是说一个群 G 总是和一个集 $M(=G)$ 上的变换群同构的．我们还知道，一个群 G 和集 M 上的一个变换群同态当且仅当 M 是一个 G－集，就是说，研究 G－集和研究群的变换群表示是一回事．

环和群的情况完全类似：有抽象环和具体环，如函数环、矩阵环、线性变换环，等等都是具体环．研究环的方法之一就是把抽象环用具体环来表示，即抽象环到某一类具体环的同态．在环论中什么相当于群论中的变换群，又是什么相当于 G－集，在环论中有没有相应于 Cayley 定理的结果？本节将讨论这些问题，而一种可能的答案是：用交换群 M 代替集 M，用交换群 M 的自同态环代替集 M 的变换群，用环 R 上的模（R－模）代替 G－集．

任取加群 M．令 End M 表示加群 M 的所有自同态的全体，规定集 End M 的加法和乘法如下：$\alpha,\beta\in\text{End }M$，$m\in M$

$$\begin{aligned}\alpha+\beta: M&\longrightarrow M\\ m&\longmapsto m\alpha+m\beta;\end{aligned}$$

$$\begin{aligned}\alpha\cdot\beta: M&\longrightarrow M\\ m&\longmapsto (m\alpha)\beta.\end{aligned}$$

直接验证可知 $\alpha\cdot\beta$ 是群 M 的自同态，注意到 M 是交换群，$\alpha+\beta$ 也是加群 M 的自同态，即有 $\alpha\cdot\beta\in\text{End }M$，$\alpha+\beta\in\text{End }M$，亦即这确是集 End M 的两个运算．直接验算可知 (End M，+，·) 是一个环，其恒等元是加群 M 的恒等

自同构 1: $\forall\ m \in M, 1: m \longmapsto m$；其零元是加群 M 的零同态 0: $\forall\ m \in M, 0: m \longmapsto 0$，称 $(\text{End } M, +, \cdot)$ 为加群 M 的自同态环. 自同态环当然是一类具体环，与矩阵（线性变换）环类似，但比之广泛得多的一类具体环.

定义 6.1 设 R 是有 1 的环，End M 是加群 M 的自同态环. 称 R 到 End M 的满足条件 $\phi(1) = 1$ 的一个同态 ϕ 为环 R 的一个（自同态环的）表示.

读者可把环的表示和群的（变换群的）表示作一对比.

定义 6.2 设 R 是有 1 的环，M 是加群，还有一个 $M \times R$ 到 M 的运算. 满足条件：$\forall\ x, y \in M, r, t \in R$，

M1) $(x + y) \cdot r = x \cdot r + y \cdot r$；

M2) $x \cdot (r + t) = x \cdot r + x \cdot t$；

M3) $x \cdot (rt) = (x \cdot r) \cdot t$；

M4) $x \cdot 1 = x$.

就称 M 为环 R 上的右模，简记作右 R - 模 M. 我们常把它看成环 R（右）作用到加群 M 上.

读者可把右 R - 模和群 G 作用于集 M 上的 G - 集作一对比：粗略地说，R - 模和 G - 集是类似的，只是前者比后者多了一个加法.

当然这和在第二章定义 8.8 中给出的 R - 模是一回事，仅有的区别是这里是定义右 R - 模，而现在该说那里是定义左 R - 模. 这和有人把元素 $x \in S$ 在集 S 的一个变换 ϕ 下的象记作 ϕx，有人记作 $x\phi$ 是类似的，本质上一样，记法不同.

下面要证明：环 R 的表示和右 R - 模是互相等价的语言. 其证明思路和我们学过的群的（变换群的）表示和 G - 集是等价的证明是完全一样的.

设 $\phi: R \to \text{End } M$ 是环 R 的一个表示. 利用 ϕ 定义环 R 到加群 M 上的一个右作用如下：对任意 $r \in R, x \in M$，有

$$x \cdot r = x\phi(r),$$

这里 $\phi(r) \in \text{End } M$ 而 $x\phi(r)$ 是 x 在 $\phi(r)$ 下的象. 直接验证可知，在这一环 R 作用下，加群 M 成为右 R - 模. 例如由于 $\phi(1) = 1$ 故有

$$x \cdot 1 = x\phi(1) = x,$$

即得 M4). 又如

$$\begin{aligned} x \cdot (r + t) &= x\phi(r + t) = x(\phi(r) + \phi(t)) \\ &= x\phi(r) + x\phi(t) = x \cdot r + x \cdot t, \end{aligned}$$

第二个等号是因为 ϕ 是环同态，第三个等号是加群的自同态的加法定义. 这就得 M2).

这样,有环 R 的一个表示,就得一个右 R －模.

今设 M 是一个右 R －模.利用右 R －模 M 定义环 R 的一个表示如下:任取 $r \in R$,规定 $\phi(r)$ 为

$$\begin{aligned}\phi(r): M &\longrightarrow M\\ x &\longmapsto x \cdot r.\end{aligned}$$

先验证 $\phi(r)$ 是加群 M 的一个自同态.这是因为对任意 $x, y \in M$,有

$$(x+y)\phi(r) = (x+y)\cdot r = x\cdot r + y\cdot r = x\phi(r) + y\phi(r).$$

这样对任意 $r \in R$,有 $\phi(r) \in \mathrm{End}\, M$.今定义对应

$$\begin{aligned}\phi: R &\longrightarrow \mathrm{End}\, M\\ r &\longmapsto \phi(r),\end{aligned}$$

而要证:ϕ 是环同态.事实上,对任意 $x \in M, r, t \in R$,有

$$\begin{aligned}x\phi(r+t) &= x\cdot(r+t) = x\cdot r + x\cdot t\\ &= x\phi(r) + x\phi(t) = x(\phi(r)+\phi(t)),\\ x\phi(rt) &= x\cdot rt = (x\cdot r)\cdot t = (x\phi(r))\cdot t\\ &= (x\phi(r))\phi(t) = x(\phi(r)\phi(t)),\end{aligned}$$

所以 $\phi(r+t) = \phi(r)+\phi(t), \phi(rt) = \phi(r)\phi(t)$,即 ϕ 是环同态,随之 ϕ 是环 R 的一个表示.

这样,有一个右 R －模,就得环 R 的一个表示.

读者不难证明:由 R 的一个表示 ϕ 出发,得一右 R －模 M,再由此右 R －模 M 又得 R 的一个表示 ψ,则有 $\phi = \psi$;类似地,由一右 R －模 M 出发,得环的一个表示 ϕ,再由此 ϕ 又得一右 R －模 N,则有 R －模 N 就是由之出发的那右 R －模 M.

上面这些事实合在一起,就说明环 R 的表示和右 R －模是一回事,是一件事情的两种表达.较之环同态 ϕ,右 R －模似乎较具体、实在、容易操作.我们已看到促使 R －模这一代数系统出现的结构理论(如有限加群的结构问题)和环表示理论的背景.这些背景已说明 R －模这一概念的重要性.

这里再重复一下 R －模的子模、商模等基本概念.我们仅对右 R －模给出,并把右 R －模简说成是 R －模.

设 M 是 R －模,N 是加群 M 的子群,如果还有 $NR \subseteq M$,就称 N 为 R －模 M 的子模,这里对任意子集 $P \subseteq M$ 和任意子集 $T \subseteq R$,规定

$$PT = \{\text{一切形如 } xt + \cdots + ys \text{ 的有限和} \mid \text{其中 } x, \cdots, y \in P, t, \cdots, s \in R\}.$$

易知 R －模 M 的子模 N 本身也是一个 R －模.

设 M 是 R －模，N 是它的一个子模.商群 $\overline{M} = M/N = \{\bar{x} = N + x, x \in M\}$ 是一个加群.今规定 R 到 $\overline{M}$ 上的(右)作用，即 $\overline{M} \times R$ 到 $\overline{M}$ 的一个运算如下：$\bar{x} \in \overline{M}, r \in R$，

$$\bar{x} \cdot r = \overline{x \cdot r}.$$

注意到 N 是子模而有性质 $NR \subseteq N$，直接验证可知上面定义与 $\bar{x}$ 的代表元 x 的选择无关，即若 $\bar{x} = \bar{y}$，则有 $\overline{xr} = \overline{yr}$.因而这个规定是合理的.不难证明它使 $\overline{M} = M/N$ 成为一个 R －模，称 R －模 M/N 为 R －模 M (关于子模 N)的商模.

两个 R －模 M 和 N，若 $\phi: M \to N$ 是加群 M 到 N 的同态，且对任意 $m \in M, r \in R$，有 $\phi(mr) = \phi(m)r$，就称 ϕ 为 R －模 M 到 R －模 N 的一个同态，如果 ϕ 还是一一对应，则称 ϕ 为 R －模 M 到 R －模 N 的同构.

如果 $\phi: M \to N$ 是 R －模同态，则 $\mathrm{Ker}\,\phi = \{m \in M \mid \phi(m) = 0\}$ 不仅是加群 M 的子群，还是 R －模 M 的子模，因为若 $m \in \mathrm{Ker}\,\phi$，则 $\phi(mR) = 0R = 0$，故也有 $mR \subseteq \mathrm{Ker}\,\phi$.和群类似的，可以证明：设 $\phi: M \to N$ 是 R －模同态，则商模 $M/\mathrm{Ker}\,\phi$ 同构于 R －模 N.证明也和群论中、环论中的类似，我们把它留给读者.

若 $N_i, 1 \leqslant i \leqslant t$，是 R －模 M 的子模，规定

$$\sum_{i=1}^{t} N_i = \{\text{一切形如 } x_1 + \cdots + x_t, x_i \in N_i, \text{的和}\}.$$

直接验证知 $\sum\limits_{i=1}^{t} N_i$ 也是子模，称之为子模 $N_i, 1 \leqslant i \leqslant t$ 的和.

定义 6.3 设 $N_1, \cdots, N_t$ 是 R －模 M 的子模.如果

(1) $M = N_1 + \cdots + N_t$ (M 的元可表成 N_i 中元的和)；

(2) 若 $0 = x_1 + \cdots + x_t, x_i \in N_i$，则必每一 $x_i = 0$ (M 的元素可表成 N_i 中元的和的唯一性)，

则称 R －模 M 为其子模 $N_1, \cdots, N_t$ 的(内)直和，记作 $M = N_1 \oplus \cdots \oplus N_t$.

设 $M_i, 1 \leqslant i \leqslant t$，都是 R －模，作加群 M_i 的直和 M，即

$$M = \{(x_1, \cdots, x_t) \mid \forall\ i, x_i \in M_i\},$$

规定 R 到 M 上的一个右作用如下：$r \in R$

$$(x_1, \cdots, x_t) \cdot r = (x_1 r, \cdots, x_t r).$$

容易验证，关于这个右作用，加群 M 成为 R －模，称之为 R －模 M_i 的(外)直和，也记作 $M = M_1 \oplus \cdots \oplus M_t$.

这里和交换群的情况完全一样，外直和与内直和是互通的，虽然本质上外

直和属于构造理论中的概念而内直和是属于结构理论的概念.

设 S 是 R - 模 M 的子集,则 S 在 R - 模 M 中生成的子模 (S),亦即 M 中含 S 的所有子模之交,恰是 SR,即 $(S)=SR$. 把它的证明留给读者.

注意到 R - 模 M 就是环 R 的一个表示,所以由一个给定 R - 模得出它的子模、商模,就相当于由一个给定的 R 的表示得出 R 的许多新的表示.类似地 R - 模的内直和相当于把环 R 的一个复杂的表示分解成 R 的一些简单的表示的"和",而 R - 模的外直和相当于由 R 的一些表示来构造出 R 的一个新的"大"表示.我们对代数系统理论的熟悉,使得在这里容易地给出诸如子模、商模、直和等概念,这比用 R 的表示这个语言去直接定义这些新表示要简单多了.

对于给定的环 R,找出它的所有表示是很难的事,有时是不可能的事,然而找到一些表示却是很容易的.和群 G 本身可看成一个 G - 集一样,环 R 本身亦可解释成为 R - 模 R,为此只要用环 R 的乘法去定义环 R 到加群 R 上的作用即得.我们称 R - 模 R 为 R - 正则模,称相应的表示为环 R 的正则表示.写出来就是下面的命题,它可和群论中的 Cayley 定理比美.

命题 6.4　带 1 的环 R 和加群 R 的自同态环 End R 的一个子环同构.这就是环 R 的正则表示.

证明　下面的推导就是找出 R - 模 R 所对应的表示.任取 $a\in R$,规定

$$\begin{aligned} R_a : R &\longrightarrow R \\ r &\longmapsto ra. \end{aligned}$$

易见 R_a 是加群 R 的一个自同态.而

$$\begin{aligned} \phi : R &\longrightarrow \text{End } R \\ a &\longmapsto R_a \end{aligned}$$

是环 R 到环 End R 的一个同态.若 $R_a=R_b$,则 $a=1R_a=1R_b=b$,即 ϕ 是单射.□

R - 模 R 的子模 T 当然给出 R 的另一新表示. $T\subseteq R$ 是子模当且仅当 T 是加群 R 的子群且 $TR\subseteq T$. 从第二个条件我们当然有 $TT\subseteq T$.

定义 6.5　设 R 是带 1 的环, $T\subseteq R$,若

1) T 是 R 的子环(不要求子环包含 R 的单位元 1)

2) $TR\subseteq T$.

就称 T 是环 R 的右理想.同样可定义环 R 的左理想.

这样, $T\subseteq R$, T 是右 R - 模 R 的子模 $\Longleftrightarrow$ T 是环 R 的右理想.因而环 R 自身带来了许多 R - 模.这就是 R 本身和 R 的右理想,例如 aR, $a\in R$,都是 R 的右理想.

在第二章§11中我们着重介绍群 G 的变换群的表示以及 G - 集，也提到群 G 的线性变换群(矩阵群)的表示以及 G - 向量空间. 这里我们把后者(群 G 的表示)和有限群 G 在域 F 上的群代数 $F[G]$ 的表示的关系交代一下. 我们将看到，这两者实际上是一回事.

定义 6.6 1) 设 G 是有限群而 M 是域 F 上有限维向量空间. 设有集 $M\times G$ 到集 M 的一个运算 ·，它满足以下条件：$\forall\ x,y\in M,\alpha\in F,g,h\in G$，

M1) $(x+y)\cdot g=x\cdot g+y\cdot g$；

M2) $(\alpha x)\cdot g=\alpha(x\cdot g)$；

M3) $(x\cdot g)\cdot h=x\cdot(gh)$；

M4) $x\cdot e=x$，其中 e 是群 G 的恒等元.

就称 M 为右 G - 向量空间，或说群 G 右作用在向量空间 M 上.

2) 称有限群 G 到域 F 上一般线性群 $GL_n(F)$ 的一个同态为群 G 的一个表示.

重复 G - 集与群 G 的变换群的表示，或 R - 模与环 R 的表示之间关系的讨论，读者容易证明：右 G - 向量空间 M 给出群 G 的一个表示，反过来也是对的，即有限群 G 的一个表示给出一个右 G - 向量空间 M.

什么是群代数 $F[G]$，或者更一般的 F 上有限维代数 A 的表示呢？对一般环 R，我们把环 R 到加群 M 的自同态环 End M 的一个同态叫作环 R 的表示. 对于代数 A，很自然地该用 F 上有限维向量空间 M 来代替加群，而得下面的

定义 6.7 1) 设 A 是有 1 的、域 F 上有限维代数，M 是 F 上有限维向量空间，还有一个集 $M\times A$ 到集 M 的运算 ·，满足条件：对任意 $x,y\in M,r,t\in A,\alpha\in F$，有

Ma) $(x+y)\cdot r=x\cdot r+y\cdot r,\quad(\alpha x)\cdot r=\alpha(x\cdot r)$；

Mb) $x\cdot(r+t)=x\cdot r+x\cdot t$；

Mc) $x\cdot(rt)=(x\cdot r)\cdot t$；

Md) $x\cdot 1=x$.

就称 M 为代数 A 上右模，简记作右 A - 模 M.

2) 称 F 上代数 A 到 F 上矩阵代数 $M_n(F)$ 的一个代数同态 ϕ 且 $\phi(1)=I$ 为代数 A 的一个表示.

如果与环 R 上模的定义 6.2 相比较，我们就会发现这里多了个要求：$(\alpha x)\cdot r=\alpha(x\cdot r)$. 我们对此该是已经习惯了：当定义 A 到 M 上的作用 · 时，我们永远要求这个作用 · 与 A 中和 M 中的所有运算都是要和谐的. 还是贯彻这个原则，读者该能给出域 F 上两个代数 A,B 的同态 ϕ 的定义：ϕ 既是环 A 到环 B 的同态，并且还是 F 上向量空间 A 到 F 上向量空间 B 的同态.

与上面完全一样，我们也有：代数 A 的表示和 A －模是一回事.

现在来看有限群 G 的(矩阵群)表示和群代数 $F[G]$ 的表示的关系.

若 $\phi: F[G] \to F_n$ 是群代数 $F[G]$ 的表示，注意到 $\phi(e) = I$，$\phi(g)\phi(g^{-1}) = \phi(e) = I$，故 $\phi(g) \in GL_n(F)$，$\forall\ g \in G$，因而把 ϕ 局限在 $F[G]$ 的子集 G 上，便得 $\phi: G \to GL_n(F)$，ϕ 当然仍保持运算，随之得 ϕ 是群 G 的一个表示.

同样地，若 M 是 $F[G]$ －模，如果我们只考虑 $F[G]$ 的子集 G 对 M 的作用，则不难证明 M 是一个 G －向量空间.

反过来，若 M 是 G －向量空间，注意到群代数 $F[G]$ 中任一元素 a 可唯一地表成

$$a = \sum_{g \in G} \alpha_g g, \quad \alpha_g \in F, \quad \forall\ g \in G.$$

今规定 $M \times F[G]$ 到 M 的运算：$m \in M$

$$m \cdot a \equiv m \cdot \Big(\big(\sum_g \alpha_g g\big)\Big) = \sum{}_g \alpha_g (m \cdot g). \tag{1}$$

直接验证，可知运算(1)使得向量空间 M 成为 $F[G]$ －模，即得 $F[G]$ －模 M.

同样地，若知群 G 的一个表示 ϕ，可得群代数 $F[G]$ 的一个表示. 可以把它看作是上一段讨论的推论，当然也可直接把 G 的一个表示 ϕ 扩大为 $F[G]$ 的一个表示.

这样群的表示和环的表示就在群和环的交叉点群代数上统一起来了.

在本节最后，让我们再一次回到第二章中有限交换群的结构定理. 在那里我们曾讨论 R 上有限生成 R －模的结构，环 R 或是整数环 $\mathbb{Z}$，或是域上一元多项式环 $F[x]$，并详细地给出 $\mathbb{Z}$－模情况的证明. 刚学过的主理想整环是 $\mathbb{Z}$ 和 $F[x]$ 的一般化，且和 $\mathbb{Z}$，$F[x]$ 非常接近. 因而把从前关于 $\mathbb{Z}$－模的结构定理的证明，平行地移到对下面定理的证明，虽有点难但并不算太难，在这里将再一次经历一下由特殊到一般的推广过程. 我们把这个工作留给读者.

关于左 R －模的一些概念可由右 R －模的概念相应得出. 当 R 是主理想整环，M 是左 R －模，$m \in M$，令 $\mathrm{Ann}(m) = \{r \in R \mid rm = 0\}$. 易知 $\mathrm{Ann}(m)$ 是 R 的理想，因而 $\mathrm{Ann}(m) = (a)$，$a \in R$，称 a 为 m 的阶. 注意，a 不是唯一的. 但最多相差 R 中的一个单位.

定理 6.8　设 R 是主理想整环，M 是有限生成左 R －模，且存在 $0 \neq r \in R$ 使得 $rM = 0$(此时称 M 为周期模)，则 R －模 M 可唯一地分解成 Rm_i，$i = 1, 2, \cdots, s$ 的直和，其中元素 m_i 的阶是 R 的素元的幂. □

下面是完整且漂亮的一个关于有限生成 R －模的结构定理. 我们略去证明. 有兴趣的读者可参看其他参考书.

定理 6.9 设 R 是主理想整环，M 是有限生成左 R－模，则 R－模 M 可唯一地分解成有限个 R－模 R 和 $Rm_i, i=1,2,\cdots,s$，的直和，其中元素 m_i 的阶是 R 的素元的幂. □

本章习题

1. 证明下列环同构：

1) $\mathbf{Z}[i]/(3+i)\cong\mathbf{Z}_{10}$.

2) $F[x]/(1+x^2)\cong\mathbf{C}$，这里 F 是数域.

2. 设环 A 仅有有限多个理想，ϕ 是 A 的满自同态，证明：ϕ 是自同构.

3.（华罗庚）设 ϕ 是环 R 到环 R' 的映射，使得对于任意 $a,b\in R$，有 $\phi(a+b)=\phi(a)+\phi(b)$ 和 $\phi(ab)=\phi(a)\phi(b)$ 或 $\phi(ab)=\phi(b)\phi(a)$. 证明：ϕ 是环同态，或者 ϕ 是环反同态（即对任意 $a,b\in R$，有 $\phi(a+b)=\phi(a)+\phi(b), \phi(ab)=\phi(b)\phi(a)$）.

4. 设 R 为交换环，N 为 R 中所有幂零元的集合，即 $N=\{a\in R\mid$ 存在 $n\in\mathbf{Z}^+$，使得 $a^n=0\}$. 证明：N 是 R 的理想，且 R/N 不含非零的幂零元.

5. 设 $\phi: R\to R'$ 是环的满同态，$K=\mathrm{Ker}\phi$. 证明：

$$R[x]/K[x]\cong R'[x].$$

6. 设 H 是四元数代数，$\{1,i,j,k\}$ 是 H 的一组 $\mathbf{R}$ 基（如§2 例 2 所述），

1) 求证：H 中元素可写为 $\alpha+\beta j$，其中 $\alpha=a+bi, \beta=c+di, a,b,c,d\in\mathbf{R}$，且 $j\alpha=\overline{\alpha}j$；

2) 令 $D=\left\{\begin{pmatrix}\alpha & \beta\\ -\overline{\beta} & \overline{\alpha}\end{pmatrix}\middle|\, \alpha,\beta\in\mathbf{C}\right\}$ 证明：D 是 $M_2(\mathbf{C})$ 的子环，且有环同构 $H\cong D$；

3) H 中由 $1,j$ 生成的子环记为 $\langle 1,j\rangle$. 求证：存在域同构 $\langle 1,j\rangle\cong\mathbf{C}$；

4) x^2+1 在 H 中有无穷多个根.

7. 设 R 是环，I 是 R 的理想，

1) 证明：$M_n(I)$ 是 $M_n(R)$ 的一个理想；

2) 证明：$M_n(R)$ 中的每个理想都具有形式 $M_n(I)$，其中 I 是 R 的一个理想.

8. 设 R 是环，I 是 R 的理想，证明：

$$M_n(R)/M_n(I)\cong M_n(R/I).$$

9.（中国剩余定理）设 $A_1,\cdots,A_n$ 是环 R 的理想，并且对任意 $i, 1\leqslant i\leqslant n$. 有 $R^2+A_i=R$，对任意 $1\leqslant i\neq j\leqslant n$，有 $A_i+A_j=R$.

1) 证明：对任意 k，$1\leqslant k\leqslant n$，有 $R=A_k+\bigcap\limits_{\substack{i=1\\ i\neq k}}^{n}A_i$.

2) 对任意给定的 $b_1,\cdots,b_n\in R$，存在 $b\in R$，使得对任意 $i, 1\leqslant I\leqslant n$，有 $b-b_i\in A_i$.

3) 对 2) 中 $b_1,\cdots,b_n\in R$，若存在 $c\in R$，$c\neq b$，且对任意 $i,1\leqslant i\leqslant n$，有 $c-$

$b_i \in A_i$，则 $b - c \in \bigcap_{i=1}^{n} A_i$.

10. 设 $m_1, \cdots, m_n$ 是正整数，且对任意 $1 \leqslant i \neq j \leqslant n$. 有 $(m_i, m_j) = 1$. 证明：如果 $b_1, \cdots, b_n \in \mathbb{Z}$，则同余方程 $x \equiv b_i (\mathrm{mod}\ m_i)$，$1 \leqslant i \leqslant n$，有整数解，并且解是由模 $m = m_1, \cdots, m_n$ 唯一确定.

11. 证明：不存在只含 6 个元素的无零因子环.

12. 设 R 是交换环，M 为 R 的极大理想，R/M 不为域，证明：$(R/M)^2 = 0$.

13. 设 A, B 是环 R 的理想，P 是 R 的素理想，$A \cap B \subseteq P$，证明：$A \subseteq P$ 或 $B \subseteq P$.

14. 设 R 是交换环，

1) P 是 R 的素理想，A 是 R 的理想，$A \cap P \neq A$，求证：$A \cap P$ 是 A 的素理想；

2) $P_1, \cdots, P_r$ 是 R 的素理想，A 是 R 的理想，且 $A \subseteq P_1 \cup \cdots \cup P_r$，证明：存在 i，$1 \leqslant i \leqslant r$，使得 $A \subseteq P_i$.

15. 在整环 $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ 中，$a = 2 + \sqrt{-5}$ 是既约元，但不是素元.

16. 在 $R = \mathbb{Z}[\sqrt{10}] = \{a + b\sqrt{10} \mid a, b \in \mathbb{Z}\}$ 中，

1) 映射 $\phi: R \longrightarrow \mathbb{Z}, a + b\sqrt{10} \longmapsto (a + b\sqrt{10})(a - b\sqrt{10}) = a^2 - 10b^2$，满足 $\phi(xy) = \phi(x)\phi(y)$，且 $\phi(x) = 0$ 当且仅当 $x = 0$；

2) x 是 R 中可逆元的充要条件是 $\phi(x) = \pm 1$；

3) $2, 4 + \sqrt{10}$ 是 R 中既约元；

4) $2, 4 + \sqrt{10}$ 不是 R 中素元；

5) R 中每个非零非单位的元素都可以分解成为既约元的乘积，但分解未必唯一.

17. 用 Zorn 引理证明：设 R 有单位元 1，A 是 R 的一个非平凡理想，则存在 R 的包含 A 的极大理想.

第四章　多项式的分裂域

本章主要讨论多项式 $f(x)$ 的分裂域,给出有限域的结构定理和 Galois 理论的基本定理.作为应用将讨论几何中三大不能问题,以及五次方程不能用根式解的问题.

§1　域

我们已有抽象域的概念,并且已接触过许多具体域,如数域 $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}(\sqrt{2})$,$\mathbb{Q}(\sqrt{2},\sqrt{3})$;有限域 $\mathbb{Z}_p$;域 F 上多项式环 $F[x]$ 的分式域 $F(x)$, $F[x_1,\cdots,x_n]$ 的分式域 $F(x_1,\cdots,x_n)$,等等.我们还知道两个获得新域的方法:一个是已知整环 R 关于其极大理想 I 的商环 R/I,一个是已知整环 R 的分式环.这是下面常用的.

域是特殊的有 1 交换环,因而关于环的一切概念,诸如子环、理想、同态等都可对域使用.说域 K 的子环 F 是 K 的子域,如果 F 本身是一个域且 F 和 K 有相同的单位元 1.与同态联系紧密的理想概念对环而言是重要的,然而对于域 F 而言它是平凡的:域 F 只有平凡理想 0 和 F.这从 F 中非零元有逆元可证得.随之,如果有环同态 $\phi: F\to R$ 而 F 是域,则由于 $\mathrm{Ker}\phi$ 或为 0 或为 F, ϕ 或是域 F 到环 R 的一个子环上的同构,或 ϕ 将整个 F 映到 0.这样,两个域 F,K 之间真正有意思的同态,只有一个,就是 F 和 K 的一个子域同构.

若 $F\subseteq K$,F,K 是域,我们称 K 是 F 的扩域,而称 F 为基本域.记作 K/F.若 K 的子域 T 介于域 F 与 K 之间,即 $F\subset T\subset K$,则称 T 为中间域.在本节中我们将讨论的问题是:扩域 K 关于基本域 F 的结构问题,以及满足一定性质的扩域 K 的存在问题.

在群论中常是给定群 G 而研究 G 的子群,如问有限群的 Sylow 子群的存在性等.在域论中,刚好相反,常是给定基本域 F 而讨论其扩域 K 的某些性质.如果考虑到,任何域都可看成素域 $\mathbb{Q}$ 或 $\mathbb{Z}_p$ 的扩域,以及我们感兴趣的分裂域 K 是 $f(x)$ 之系数所在域 F 的扩域,这样,域论中的主要概念都是相对于一个取定的基本域 F 而引入的.如果已知 K 是 F 的扩域,我们只对中间域感兴趣.

设 K 是域 F 的一个扩域，S 是 K 的一个子集，我们用 $F(S)$ 表示 K 的含 $F\cup S$ 的最小子域，称为把 S 添加到基本域 F 上而得到的中间域. 下面看一下 $F(S)$ 是由什么样的一些元素组成的.

设 $F[S]$ 表示一切 F 上以 S 中元素为“变元”的多项式

$$\sum f_\alpha s_1^{n_1}\cdots s_m^{n_m} \quad \forall\ s_i\in S, m\in\mathbb{Z}^+\cup\{0\} \tag{1}$$

的全体. 这里 $\alpha=(n_1,\cdots,n_m)\in\mathbb{Z}^{+m}$, $f_\alpha\in F$，直接验证知 $F[S]$ 是 K 的子环，显然 $F[S]\subseteq F(S)$. 设

$$T=\{uv^{-1}\mid u,v\in F[S],v\neq 0\}, \tag{2}$$

易见 $T\subseteq F(S)$. 另一方面易知 T 是子域，$F\subseteq T$, $S\subseteq T$，故由 $F(S)$ 是含 $F\cup S$ 的最小子域，得 $F(S)\subseteq T$. 故得 $F(S)=T$. 这样 $F(S)$ 是由形如(2)的元素组成的，即 $F(S)$ 是由 F 上 S 的“有理式”组成的.

命题 1.1 $F\subseteq K$, F,K 是域，$S_1\subseteq K$, $S_2\subseteq K$. 则有

$$F(S_1)(S_2)=F(S_1\cup S_2).$$

这个结论用语言表达就是：先把 S_1 添加到 F 上，然后再把 S_2 添加到 $F(S_1)$ 上去，就等于把 $S_1\cup S_2$ 一下子添加到 F 上去. 想起来，这当然是对的. 但要证明它，只能严格按照它们的定义去推导.

证明 显然 F,S_1,S_2 含在域 $F(S_1)(S_2)$ 内，另一方面，$F(S_1\cup S_2)$ 是含 $F,S_1\cup S_2$ 的最小子域，故有 $F(S_1\cup S_2)\subseteq F(S_1)(S_2)$. 类似地可证，$F(S_1)(S_2)\subseteq F(S_1\cup S_2)$. 两个包含关系合起来，便得要证的结论. □

利用这个生成元集 S，可对扩域作如下的分类.

定义 1.2 当 S 是有限集时，称 $K=F(S)$ 为 F 的有限生成扩域. 当 $S=\{a\}$ 是一个元素时，称 $F(a)$ 为 F 的单扩域.

由上命题知：$F(a_1,a_2,\cdots,a_n)=F(a_1)(a_2)\cdots(a_n)$，即有限生成扩域可归结为在一些域上连续作单扩域.

当 $F\subseteq K$ 时，可把 K 自然地解释成为域 F 上的一个向量空间：$(K,+)$ 是一个加群而数乘运算 $a\cdot\alpha$, $a\in F$, $\alpha\in K$，就用域 K 中的乘法. 直接验证知 F - 向量空间的一切要求都是满足的. 扩域 K 是基本域 F 上的向量空间，这样我们就可把向量空间的知识、概念拿来自由使用了. 将用 $[K:F]$ 表示 F - 向量空间 K 的维数. 从这个角度，又可对扩域进行分类.

定义 1.3 当 $[K:F]=n$ 时，称 K 为 F 的 n 次扩域；当 $[K:F]=\infty$ 时称 K 为 F 的无限次扩域. 称 $[K:F]$ 为扩域 K 的 F - 次数(或简称次数).

关于扩域 K 的次数，有下面常用到的基本事实.

命题 1.4 设 $F\subseteq H\subseteq K$, F,H,K 都是域，则有

$$[K:F]=[K:H][H:F].$$

证明 设 $[K:H]=n,[H:F]=m$. 设 $k_1,\cdots,k_n$ 是 H - 向量空间 K 的一个基，$h_1,\cdots,h_m$ 是 F - 向量空间 H 的一个基. 今证 $h_ik_j, 1\leqslant i\leqslant m, 1\leqslant j\leqslant n$，是 F - 向量空间 K 的一个基. 容易看到它们是 F - 向量空间 K 的一个生成元集. 它们还是 F - 线性无关的，这是因为，若有 $a_{ij}\in F$ 使 $\sum_{i,j}a_{ij}h_ik_j=0$，则由

$$\sum_j\Big(\sum_i a_{ij}h_i\Big)k_j=0,\quad \sum_i a_{ij}h_i\in H,$$

以及 $\{k_j\}$ 是 H - 线性无关的，得到对所有 j，

$$\sum_i a_{ij}h_i=0,\quad a_{ij}\in F.$$

注意到 $\{h_i\}$ 是 F - 线性无关的，由上式便得对任意 i,j，有 $a_{ij}=0$. 这样就证明了 $\{h_ik_j\}$ 是 F - 向量空间 K 的一个基. □

研究扩域 K 的结构，考虑 K 中元素相对于基本域 F 的性质是重要的. 这里自然的样板是代数数和超越数的概念，即复数相对于有理数域 $\mathbf{Q}$ 的一种分类.

定义 1.5 $F\subseteq K, F, K$ 是域.

a) 称 $\alpha\in K$ 是 F 上代数元，如果有非零多项式 $f(x)\in F[x]$，使 $f(\alpha)=0$，这也就是说，存在自然数 n，使得

$$1,\alpha,\alpha^2,\cdots,\alpha^n$$

是 F - 线性相关的. 并称 α 所满足的 $F[x]$ 中次数最小的多项式 $g(x)$ 为 α 在 F 上的极小多项式. 还称 $g(x)$ 的次数为代数元 α 的 F - 次数.

b) 称 $\alpha\in K$ 为 F 上超越元，如果 α 不是代数元，亦即

$$1,\alpha,\cdots,\alpha^n,\cdots$$

是 F - 线性无关的.

我们知道，$F[x]$ 上正次数多项式 $p(x)$ 称为不可约的，是指它不能分解为两个正次数多项式的乘积. 不可约多项式即为整环 $F[x]$ 中的既约元. 容易证明：代数元在 F 上的极小多项式是不可约的. 并且，若 $f(x), g(x)$ 是 α 在 F 上的极小多项式，则存在 $0\neq a\in F$，使得 $f(x)=ag(x)$.

显然，代数数是 $\mathbf{Q}$ 上的代数元，而超越数 e,π 是 $\mathbf{Q}$ 上的超越元.

从这个元素分类的角度，我们有下面对扩域的分类.

定义 1.6 $F\subseteq K, F, K$ 是域. 如果 $K\setminus F$ 中元(这也就是说 K 中所有元)都是 F 上代数元，就称 K 为 F 的代数扩域. 如果 $K\setminus F$ 中存在 F 的超越元，就称 K 为 F 的超越扩域.

与定义 1.3 比较一下是有益的. 在那里强调 K 是 F - 向量空间,但这并没有用上域 K 中的全部运算,因而扩域 K 的 F - 次数概念涉及 K 的结构不多,是一种工具性的概念,而代数扩域和超越扩域概念则较深入地涉及扩域的结构性质.

在本节最后我们汇集任意域上一元多项式及其根的性质.

我们熟悉数域上一元多项式及其根的性质. 然而这些性质对有限域以及特征 p 的域,是否成立? 还是应该仔细讨论的.

对于数域 F 上的一元多项式 $f(x)$, 数 $a \in F$ 是 $f(x)$ 的重根(即 $(x-a)^2$ 整除 $f(x)$)当且仅当 $f(a) = f'(a) = 0$, 其中 $f'(x)$ 是 $f(x)$ 的导数. 虽然在一般域 F 上的 $F[x]$ 中我们尚没有极限的概念,但仍可形式地引进如下

定义 1.7 $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in F[x]$, F 是任意域. 规定

$$f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + 2a_2 x + a_1.$$

其中 $n, n-1, \cdots, 2, 1$ 等看做是 F 中的元素. 称 $f'(x)$ 为 $f(x)$ 的导式.

直接验证可知,这里也有: $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$, $(f(x) + g(x))' = f'(x) + g'(x)$.

但能否用这个形式的导式 $f'(x)$ 来判断 $f(x)$ 有无重根,则是需要证明的. 下面命题列出一般域上一元多项式及其根的性质.

命题 1.8 F 是任意域.

1) $F[x]$ 是 Euclid 环.

2) 设 $f(x), g(x), h(x) \in \mathbb{Z}[x]$, 若在 $\mathbb{Z}[x]$ 中 $f(x) = g(x)h(x)$, 则在 $F[x]$ 中(把这些多项式 $f(x), g(x), h(x)$ 的整数系数看作是 F 的素子域中的元素)也有 $f(x) = g(x)h(x)$.

3) $f(x) \in F[x]$, $a \in F$. 则 $f(a) = 0$ 当且仅当 $(x-a) \mid f(x)$.

4) n 次多项式 $f(x) \in F[x]$. $f(x)$ 在 F 中最多有 n 个不同的根.

5) 设 $f(x) \in F[x]$, E 是 F 的扩域. 设 $a \in E$, 则 a 是 $f(x)$ 的重根(即在 $E[x]$ 上 $(x-a)^2 \mid f(x)$)当且仅当 $f(a) = f'(a) = 0$.

6) 设 $f(x), g(x) \in F[x]$, $f(x)$ 是不可约的. 如果 $f(x), g(x)$ 在 F 的一个扩域 E 中有公共根,则在 $F[x]$ 中有 $f(x) \mid g(x)$.

7) $f(x) \in F[x]$, F 的特征为 0, $f(x)$ 是不可约多项式,则 $f(x)$ 无重根.

8) $f(x), g(x) \in F[x]$, F 的特征为素数 p, 则有 $(f(x) + g(x))^p = f(x)^p + g(x)^p$.

证明 证 2). 这是因为

$$\phi: \mathbb{Z}[x] \longrightarrow F[x]$$
$$f(x) \longmapsto f(x)$$

在 F 之特征为 0 时是到 $F[x]$ 的子环 $\mathbb{Z}[x]$ 上的同构,而在 F 之特征为 p 时是到 $F[x]$ 的子环 $\mathbb{Z}_p[x]$ 上的同态. 故得 2).

证 3). 在 $F[x]$ 中有 $x^n - a^n = (x-a)(x^{n-1} + ax^{n-2} + \cdots + a^{n-1})$. 故对多项式 $f(x) = \sum a_i x^i$, 若 $f(a) = 0$, 则 $f(x) = f(x) - f(a) = \sum_{i>0} a_i(x^i - a^i) = (x-a)\sum a_i(x^{i-1} + ax^{i-2} + \cdots + a^{i-1})$. 故得 3).

4)是 3)的推论.

今证 5). $f(x) \in F[x] \subseteq E[x]$. 设 a 是 $f(x)$ 的根,则由 3), $f(x) = (x-a)g(x)$, a 是 $f(x)$ 的重根当且仅当 a 是 $g(x)$ 的根. 由 $f'(x) = (x-a)g'(x) + g(x)$ 知 a 是 $g(x)$ 的根当且仅当 a 是 $f'(x)$ 的根,故得 5).

6) $f(x), g(x)$ 在 E 上有公共根 α, 设 α 在 F 上有极小多项式 $h(x)$, 则在 $F[x]$ 上, $h(x) \mid f(x), h(x) \mid g(x)$. 由于 $h(x), f(x)$ 在 $F[x]$ 上是不可约的,所以 $f(x)$ 与 $h(x)$ 相伴,所以 $f(x) \mid g(x)$.

7) 设 $f(x)$ 在 F 的一个扩域 E 上有重根 α; 由 5)知 $f(\alpha) = f'(\alpha) = 0$. 而 $f'(x) \in F[x]$. 再由 6)知 $f(x) \mid f'(x)$. 比较两者次数即得 $f'(x) = 0$, 即 $f(x)$ 是常数多项式. 这与 $f(x)$ 不可约矛盾.

最后证 8). 由 2)二项式定理仍成立. 注意到 $(a+b)^p$ 之展开式中除 a^p, b^p 外,其他各项系数都是素数 p 的倍数,在特征为 p 的域中,这些系数都为零,故得 8). □

练习

1. 证明:有限次扩域是代数扩域.
2. 若域扩张 K/F 的次数 $[K:F]$ 为素数 p, 则 K/F 没有非平凡的中间域.
3. 设 K/F 是有限次扩域,且 $[K:F]$ 为素数 p. 设 $\alpha \in K$ 且 $\alpha \notin F$, 则 $K = F(\alpha)$.
4. 考虑域扩张 $\mathbb{Q}(\sqrt{2}+\sqrt{3})/\mathbb{Q}$,
   1) 求扩张次数 $[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}]$;
   2) 写出 $\mathbb{Q}(\sqrt{2}+\sqrt{3})/\mathbb{Q}$ 的所有中间域,并求这些中间域在 $\mathbb{Q}$ 上的次数;
   3) 证明: $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$.
5. 设 K/F 是代数扩域, $\alpha \in K$, 则存在 $f(x) \in F[x]$, 使得 $\alpha^{-1} = f(\alpha)$.
6. 设 K/F 是代数扩域, L, M 是中间域,求证:

$$LM = \left\{ \sum_{i=1}^{n} l_i m_i \,\middle|\, n \in \mathbb{Z}^+, l_i \in L, m_i \in M, 1 \leqslant i \leqslant n \right\}$$

是 K/F 的中间域.

§2 分裂域

我们先来讨论最基本的扩域——单扩域.

命题 2.1 1) 如果 $K = F(\alpha)$，而 α 是 F 上代数元，$p(x)$ 是 α 在 F 上的极小多项式，则 $K = F(\alpha) \cong F[x]/(p(x))$，其中 $F[x]$ 是 F 上一元多项式环.

2) 设 $\deg p(x) = n$，则 $F(\alpha)$ 中每一个元素都可以唯一表成

$$\sum_{i=0}^{n-1} a_i\alpha^i, \quad a_i \in F$$

的形式. 这样的两个多项式 $f(\alpha)$ 与 $g(\alpha)$ 相加，只需把相应的系数相加；$f(\alpha)$ 与 $g(\alpha)$ 的乘积等于 $r(\alpha)$，这里 $r(x)$ 是 $p(x)$ 除 $f(x)g(x)$ 所得的余式. 特别地，$1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ 是 $F(\alpha)$ 作为 F - 空间的基，因而有 $[F(\alpha):F] = n$.

3) 对任意给定域 F 和任意给定的不可约多项式 $p(x)$，总存在单扩域 $K = F(\alpha)$，α 是 F 上代数元，且 $p(x)$ 是 α 的 F - 极小多项式.

证明 1) 考虑对应

$$\begin{aligned} \phi: F[x] &\longrightarrow F(\alpha) \\ f(x) &\longmapsto f(\alpha), \end{aligned}$$

易知 ϕ 是环 $F[x]$ 到环 $F(\alpha)$ 的环同态. $\mathrm{Ker}\phi = (p(x))$，这是因为 $f(\alpha) = 0$ 当且仅当 $p(x) \mid f(x)$. 这样 ϕ 诱导出下面同构(仍记作 ϕ)：

$$\phi: F[x]/(p(x)) \cong \mathrm{Im}\phi \subseteq F(\alpha).$$

由于 $F[x]/(p(x))$ 是域(见第三章)，故与之同构的 $\mathrm{Im}\phi$ 也是域. 另一方面 $\alpha = \phi(x) \in \mathrm{Im}\phi$，$F = \phi F \subseteq \mathrm{Im}\phi$，即 $\mathrm{Im}\phi$ 是包含 $F \cup \alpha$ 的子域，但 $F(\alpha)$ 是有此性质的最小域，故 $F(\alpha) \subseteq \mathrm{Im}\phi$，因而有 $\mathrm{Im}\phi = F(\alpha)$. 从而证得 1).

2) 因 $\mathrm{Im}\phi = F(\alpha)$，故 $F(\alpha)$ 的任意元 β 可写成

$$\beta = h(\alpha) = \sum_i b_i\alpha^i, \quad b_i \in F$$

的形式，但 $h(x) = p(x)q(x) + r(x)$，其中 $r(x) = \sum_{i=0}^{n-1} a_ix^i$，$a_i \in F$. 因而由于 $p(\alpha) = 0$，有

$$\beta = h(\alpha) = r(\alpha) = \sum_{i=0}^{n-1} a_i\alpha^i.$$

这种表示是唯一的，因为设

$$\beta = r_1(\alpha) = r_2(\alpha), \quad \deg r_i(x) < n \quad 或 \ r_i(x) = 0 (i = 1,2)$$

则 $r_1(\alpha)-r_2(\alpha)=0$, 所以 $p(x)\mid r_1(x)-r_2(x)$. 因 $p(x)$是 α 的极小多项式,故 $r_1(x)-r_2(x)=0$. 即 $r_1(x)=r_2(x)$.

从以上证明可以看出,2)中其余部分成立.

3) 由给定的域 F 及 $p(x)\in F[x]$, 我们可以构造商环 $K=F[x]/(p(x))$. 令 $\bar{x}=x+(p(x))$, 而考察满同态对应

$$\phi: F[x]\longrightarrow K=F[x]/(p(x))$$
$$f(x)\longmapsto f(\bar{x}).$$

特别地,对任意 $a\in F$, 有 $\phi(a)=a+(p(x))$, 且 $\phi(x)=x+(p(x))$. 注意到在 ϕ 下 F 和 $\bar{F}=\{\bar{a},a\in F\}$ 是同构的,(证明!)在 K 中把 $\bar{a}$ 改写成 a, 或者说按同构 ϕ 把 $\bar{F}$ 和 F 等同起来,这样就有 $F=\bar{F}\subseteq K$. 这样

$$K=\{f(\bar{x}),f(x)\in F[x]\}=F[\bar{x}].$$

由于 $p(x)$ 是 F - 不可约多项式,故 K 是域,另一方面,对 $f(x)\in F[x]$, $f(\bar{x})=0$ 当且仅当 $p(x)\mid f(x)$, $p(x)$ 是 $\bar{x}$ 的一个 F - 极小多项式. 总起来便得 K 是把 $\alpha=\bar{x}$ 添加到 F 而得的扩域,其中 $p(x)$ 是 α 的极小多项式. □

例 1 设 $f(x)=x^3-2\in\mathbb{Q}[x]$, $f(x)$ 在 $\mathbb{R}$ 上有一个根 $\alpha=\sqrt[3]{2}$, 则 $\mathbb{Q}(\sqrt[3]{2})=F[x]/(x^3-2)$. $\mathbb{Q}(\sqrt[3]{2})$ 中的元素可唯一表为 $a_0+a_1\sqrt[3]{2}+a_2\sqrt[3]{4}$ 的形式,其中 $a_0,a_1,a_2\in\mathbb{Q}$. 而 $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3$.

用上面证明的思路,可以证明下面

命题 2.2 1) 如果 $K=F(\alpha)$ 而 α 是域 F 上超越元,则

$$K=F(\alpha)\cong F(x),$$

其中 $F(x)$ 是 F 上一元多项式环 $F[x]$ 的分式域.

2) 对任意域 F, 总存在单扩域 $K=F(\alpha)$, α 是 F 上超越元. □

由命题 2.1,用一下归纳法便得

命题 2.3 设 $K=F(S)$, 其中 $S=\{\alpha_1,\cdots,\alpha_m\}$, 且 α_i 是 F 上次数为 n_i 的代数元,则有 $[F(S):F]\leqslant n_1n_2\cdots n_m$.

证明 我们只考察 $F(\alpha,\beta)=F(\alpha)(\beta)$ 的情况. 设 $p(x)$ 是 β 的 F - 极小多项式. 由 $p(x)\in F(\alpha)[x]$, $p(\beta)=0$ 知 β 是 $F(\alpha)$ 上代数元且

$$\beta \text{ 的 } F(\alpha)-\text{次数}\leqslant\beta \text{ 的 } F-\text{次数}=n_2,$$

这样便得

$$[F(\alpha,\beta):F]=[F(\alpha)(\beta):F(\alpha)][F(\alpha):F]\leqslant n_1n_2. \qquad □$$

设 $f(x)\in F[x]$, 如果在 F 的扩域 E 上 $f(x)$ 可以完全分解, $f(x)=a(x-\alpha_1)\cdots(x-\alpha_n)$, 把 $\alpha_1,\cdots,\alpha_n$ 添加到基域 F 上而得扩域 $K=F(\alpha_1,\cdots,\alpha_n)$, 这样这些根就有了一个活动的空间,也就更便于研究它们. 把一元多项式 $f(x)$ 和一个域 $F(\alpha_1,\cdots,\alpha_n)$ 联系是一个非常自然而有益的方法.

当 F 是数域，我们有一个复数域 $\mathbb{C}$，使 $F \subseteq \mathbb{C}$. 注意到 $\mathbb{C}$ 是代数闭域，即 $\mathbb{C}$ 上任一正次数的多项式 $f(x)$，在 $\mathbb{C}$ 中必有根，即在 $\mathbb{C}[x]$ 中，$f(x) = a(x-\alpha_1)\cdots(x-\alpha_n)$. 把 F 的扩域 $\mathbb{C}$ 中元素 $\alpha_1,\cdots,\alpha_n$ 添加到数域 F 上就得到我们所想有的扩域 $F(\alpha_1,\cdots,\alpha_n)$.

但如果 F 是一般的域，例如有限域，则目前我们尚不知 F 的扩域中是否有一个代数闭域，因而扩域 $F(\alpha_1,\cdots,\alpha_n)$ 的存在性就是个问题了.

本节将解决这一问题. 这是对一般域理论以及有限域的结构理论的非常重要的准备.

定义 2.4　F 是域，正次数的 $f(x) \in F[x]$. 如果在 F 的一个扩域 K 中，$f(x)$ 完全分解，即有 $f(x) = a(x-\alpha_1)\cdots(x-\alpha_n)$，$\alpha_i \in K$，$1 \leqslant i \leqslant n$，则称 K 的子域 $F(\alpha_1,\cdots,\alpha_n)$ 为 F 上多项式 $f(x)$ 的一个分裂域（或 $f(x)$ 在域 F 上的一个分裂域），简称 $F(\alpha_1,\cdots,\alpha_n)$ 是 F 的一个分裂域.

例 2　设 $f(x) = x^3 - 2 \in \mathbb{Q}[x]$，$f(x)$ 在 $\mathbb{C}$ 上有分解式 $x^3 - 2 = (x-\sqrt[3]{2})(x-\sqrt[3]{2}\omega)(x-\sqrt[3]{2}\omega^2)$，这里 $\omega = \frac{1}{2}(-1+i\sqrt{3})$. 故 $f(x)$ 在 $\mathbb{Q}$ 上的分裂域为 $\mathbb{Q}(\sqrt[3]{2},\sqrt[3]{2}\omega,\sqrt[3]{2}\omega^2) = \mathbb{Q}(\sqrt[3]{2},\omega)$.

从上述定义来看，一般域 F 上 $f(x)$ 的分裂域的存在性是个问题，且对任意域（包括数域）而言，$f(x)$ 的分裂域的唯一性也是个待解决的问题.

定理 2.5（分裂域的存在定理）　F 是域，正次数多项式 $f(x) \in F[x]$ 的分裂域是存在的.

证明　用归纳法要证的命题是："对任意域 K（不只是对 F），n 次多项式 $g(x) \in K[x]$ 的分裂域是存在的". 当 $n = 1$，一次多项式 $g(x) = c(x-\alpha)$，$\alpha \in K$，此时 $K(\alpha) = K$ 就是 $g(x)$ 的分裂域. 对任意 $n > 1$，n 次多项式 $g(x) \in K[x]$ 或是 K 上可约的或是 K 上不可约的. 在第一种情形 $g(x) = g_1(x)g_2(x)$，　$1 \leqslant g_i(x)$ 的次数 $< n$，$i = 1,2$. 由归纳法假设 K 上多项式 $g_1(x) \in K[x]$ 有分裂域 $K_1 = K(\alpha_1,\cdots,\alpha_s)$，　α_j 是 $g_1(x)$ 的全部根，K_1 上多项式 $g_2(x) \in K_1[x]$ 有分裂域 $K_2 = K_1(\beta_1,\cdots,\beta_t)$，$\beta_j$ 是 $g_2(x)$ 的全部根. 这样

$$\begin{aligned} K_2 &= K_1(\beta_1,\cdots,\beta_t) = K(\alpha_1,\cdots,\alpha_s)(\beta_1,\cdots,\beta_t) \\ &= K(\alpha_1,\cdots,\alpha_s,\beta_1,\cdots,\beta_t) \end{aligned}$$

便是 $g_1(x)g_2(x) = f(x) \in K[x]$ 的分裂域.

若是第二种情形，即 $g(x)$ 是 K 上不可约多项式. 此时作 K 的扩域 $K_1 = K[x]/(g(x))$ 而知 $\exists\, \alpha(=\bar{x}) \in K_1$ 有 $g(\alpha) = 0$. 随之在 $K_1[x]$ 中，有

$$g(x) = (x-\alpha)\cdot g_1(x).$$

这时 $g_1(x) \in K_1[x]$ 且其次数 $< n$. 由归纳法假设，K_1 上多项式 $g_1(x)$ 有

分裂域 $K_2 = K_1(\beta_1,\cdots,\beta_{n-1})$. 这样

$$K_2 = K_1(\beta_1,\cdots,\beta_{n-1}) = K(\alpha)(\beta_1,\cdots,\beta_{n-1}) = K(\alpha,\beta_1,\cdots,\beta_{n-1})$$

便是 $g(x) \in K[x]$ 的分裂域.□

定义 2.6 称域 F 的两个扩域 K_1, K_2 是 F 的扩域同构,如果有域同构 $\phi: K_1 \to K_2$,且此域同构 ϕ 保持 F 中元素不变,即对任意 $a \in F$,有 $\phi(a) = a$. 此时,记 ϕ 为 F - 同构.

读者在这里复习一下第一章的定义 2.8 是有益的.

这样,多项式 $f(x) \in F[x]$ 的分裂域的唯一性是指,$f(x)$ 的任意两个分裂域必是 F - 同构的. 为此先作一点准备.

命题 2.7 1) 设 $\phi: F \to \overline{F}$ 是域同构,则存在环同构 $\psi: F[x] \to \overline{F}[x]$,使得 $\psi|_F = \phi$. 又设 $p(x)$ 是 $F[x]$ 上不可约多项式,则 $\psi(p(x)) = \overline{p}(x)$ 也是 $\overline{F}[x]$ 的不可约多项式.

2) 设 $\phi: F \to \overline{F}$ 是域同构,$p(x) \in F[x]$ 是不可约多项式,在 1)的意义下,$\overline{p}(x)$ 是 $\overline{F}[x]$ 中不可约多项式,设 $F(\alpha)$ 与 $\overline{F}(\overline{\alpha})$ 分别是 F 与 $\overline{F}$ 的单扩域,满足 $p(\alpha) = 0, \overline{p}(\overline{\alpha}) = 0$,那么存在域同构 $\varphi: F(\alpha) \to \overline{F}(\overline{\alpha})$,使得 $\varphi(\alpha) = \overline{\alpha}$, $\varphi|_F = \phi$.

证明 1) 定义

$$\begin{aligned} \psi: F[x] &\longrightarrow \overline{F}[x] \\ \sum a_i x^i &\longmapsto \sum \phi(a_i) x^i, \end{aligned}$$

则可以直接验证.

2) 设 $p(x)$ 的次数为 n,则 $\overline{p}(x)$ 的次数也是 n. 令

$$\begin{aligned} \phi: \quad F(\alpha) &\longrightarrow \overline{F}(\overline{\alpha}) \\ \sum_{i=0}^{n-1} a_i \alpha^i &\longmapsto \sum_{i=0}^{n-1} \phi(a_i) \overline{\alpha}^i, \end{aligned}$$

可直接验证结论成立. 验证时要注意 $F(\alpha)$ 与 $\overline{F}(\overline{\alpha})$ 中的乘法法则.□

定义 2.8 已知域同构 $\phi: F \to \overline{F}, \psi: K \to \overline{K}, F \subseteq K, \overline{F} \subseteq \overline{K}$. 若 $\psi|_F = \phi$,则称域同构 ψ 为域同构 ϕ 的一个开拓,也说将 ϕ 开拓成 ψ.

为了证明分裂域的唯一性,只需证明下面

命题 2.9 $\phi: F \to \overline{F}$ 是域同构,$F[x]$ 中的 $f(x)$ 与 $\overline{F}[x]$ 中的 $\overline{f}(x)$ 是命题 2.7 意义下相对应的 n 次多项式,设 $K = F(\alpha_1,\cdots,\alpha_n)$ 是 $f(x)$ 在 F 上的分裂域,K 和 $\overline{f}(x) \in \overline{F}[x]$ 在 $\overline{F}$ 上的分裂域 $\overline{K}$ 间必有同构 $\psi: K \to \overline{K}$ 且 $\psi|_F = \phi$.

显然取 $F = \overline{F}$,取 ϕ 为 F 的恒等自同构,由命题 2.9 即得分裂域的唯一性. 之所以给命题 2.9,是出于归纳法证明的需要.

如果我们能选择 $\bar{f}(x)$ 的根 β_1 是与 $f(x)$ 的根 α_1 的"相应者"，即使 $F(\alpha_1)\cong\overline{F}(\beta_1)$，这时又知 $\overline{K}=\overline{F}(\beta_1)(\beta_2,\cdots,\beta_n)$，利用命题 2.7 及归纳法假设，即可得证得命题．可以对次数 $[K:F]$ 作归纳法，也可以对 $f(x)$ 的次数 n 作归纳法．我们给出后者的证明，而将前者的证明留给读者作练习．

证明 对 $f(x)$ 的次数 n 作归纳．当 $f(x)$ 的次数 $n=1$，随之 $\bar{f}(x)$ 的次数也是 1，这时

$$x-\alpha_1\in F[x],\quad x-\beta_1\in\overline{F}[x],$$

即 $K=F(\alpha_1)=F,\overline{K}=\overline{F}(\beta_1)=\overline{F}$．这种情形命题显然成立．

设 $f(x)$ 的次数 $n>1$．若 $f(x)$ 的不可约因式都是一次的，随之 $\bar{f}(x)$ 也是，此时 $K=F$ 而 $\overline{K}=\overline{F}$，命题成立．设 $f(x)=p(x)\cdot f_1(x)$，这里 $p(x)$ 是次数 $t>1$ 的不可约多项式，随之 $\bar{f}(x)=\overline{p}(x)\cdot\overline{f_1}(x)$．不妨设 $p(\alpha_1)=0$ 及 $\overline{p}(\beta_1)=0$．令 $K_1=F(\alpha_1),\overline{K_1}=\overline{F}(\beta_1)$．依命题 2.7 之 2)有域同构 $\psi:F(\alpha_1)\to\overline{F}(\beta_1),\psi|_F=\phi$．

考察域同构 $\psi:F(\alpha_1)\to\overline{F}(\beta_1)$ 及扩域 $K/F(\alpha_1),\overline{K}/\overline{F}(\beta_1)$．在 $F(\alpha_1)$ 中 $f(x)=(x-\alpha_1)\cdot g_1(x)$，在 $\overline{F}(\beta_1)$ 中 $\bar{f}(x)=(x-\beta_1)\cdot\overline{g_1}(x)$，其中 $\overline{g_1}(x)=\psi g_1(x)$．这样 K 可看成 $g_1(x)$ 在 $F(\alpha_1)$ 上的分裂域，$\overline{K}$ 可看成 $\overline{g_1}(x)$ 在 $\overline{F}(\beta_1)$ 上的分裂域．但 $g_1(x)$ 之次数是 $n-1$．由归纳法假设知必有域同构 $\Sigma:K\longrightarrow\overline{K},\Sigma|_{F(\alpha_1)}=\psi$，随之 $\Sigma|_F=\phi$．至此命题证完．□

把上面的结果写在一起就是下面

定理 2.10 F 是任意域，，则 $F[x]$ 中的正次数多项式 $f(x)$ 在 F 上的分裂域是存在的，且在 F－同构的意义下是唯一的．

练习

1．设 E/F 是域扩张．$\alpha,\beta\in E$ 是 F 上的代数元，证明：$\alpha\pm\beta,\alpha\beta,\alpha\beta^{-1}$ $(\beta\neq0)$ 均为 F 上代数元．

2．证明：域 $\mathbf{Q}(\sqrt{-1})$ 和域 $\mathbf{Q}(\sqrt{2})$ 不同构．

3．证明：$\mathbf{Q}$ 上多项式 x^4+1 的分裂域是一个单扩域 $\mathbf{Q}(\alpha)$，其中 α 是 x^4+1 的一个根．

4．1) $\mathbf{Q}(\sqrt[3]{2})$ 是不是 x^3-2 在 $\mathbf{Q}$ 上的分裂域？

2) 设 F 的特征为 p，$F(\mu)$ 是 F 的单扩域，使得 μ 是 $F[x]$ 中多项式 x^p-a 的一个根．问 $F(\mu)$ 是不是 x^p-a 的分裂域？

5．设 $f(x)$ 是域 F 上任意 n 次多项式 $(n>0)$，证明：$f(x)$ 的分裂域 K 对于 F 的次数 $[K:F]\leqslant n!$．

6．1) 求 $\sqrt{3}+\sqrt{5}$ 在 $\mathbf{Q}$ 上的一个极小多项式 $p(x)$．

2) 求 1)中 $p(x)$ 在 $\mathbb{C}$ 中的分裂域.

§3 有限域(分裂域的一个应用)

有限域是一类重要的代数系统.有限域在有限几何中起的作用和实数域在解析几何中起的作用类似,有限域在有限数学、编码理论中有重要应用,关于后者,我们将在§9中作一初步介绍.本节中将给出有限域的存在性以及初步的结构.

有限域 F 的特征当然是素数 p,因而包含素域 $\mathbb{Z}_p$. 这样 F 是 $\mathbb{Z}_p$ 上有限维向量空间,说是 n 维,随之 F 的元素个数 $|F| = p^n$.

命题 3.1 1) 有限域 F 的元素个数是 p^n, p 是它的特征数.

2) 扩域 $F/\mathbb{Z}_p$ 可看成多项式 $x^{p^n} - x$ 在 $\mathbb{Z}_p$ 上的分裂域.

证明 今证 2). 由 1)知以 F 中乘法为运算的交换群 $(F\setminus\{0\},\cdot)$ 的阶为 $p^n - 1$, 随之, F 中非零元 x 满足方程

$$x^{p^n-1} = 1,$$

因而 F 中任意元(包括零元) x 满足方程

$$x^{p^n} = x.$$

这等于说 F 中任意元 x 都是 $\mathbb{Z}[x]$ 中多项式

$$f(x) = x^{p^n} - x \tag{1}$$

的根.但一个域上的 m 次多项式在其任意扩域上最多有 m 个不同的根,因而 F 中 p^n 个元素恰好是 $f(x)$ 的全部根,即在 F 上

$$f(x) = x(x-\alpha_2)\cdots(x-\alpha_{p^n}),\quad \alpha_i \in F,$$

这就证明了 F 是 $f(x)$ 在 $\mathbb{Z}_p$ 上的分裂域.□

上命题是说,如果元素个数为 p^n 的有限域存在的话,它必是(1)中 $f(x)$ 在 $\mathbb{Z}_p$ 上的分裂域.这提示我们,构造有限域不必考虑别的多项式,只考虑(1)中 $f(x)$ 在 $\mathbb{Z}_p$ 上的分裂域就够了.

命题 3.2 多项式 $f(x) = x^{p^n} - x$ 在 $\mathbb{Z}_p$ 上的分裂域 F 的元素个数是 p^n.

证明 $f(x)$ 的导式

$$f'(x) = p^n x^{p^n-1} - 1 = -1.$$

故 $f'(x)$ 在 F 的任意扩域上没有根,由命题 1.8 之 5)知, $f(x)$ 无重根.设其 p^n 个根为 $\{\alpha_i \mid 1 \leqslant i \leqslant p^n\} = T \subseteq F$. 今证 T 是 F 的一个子域.

设 $\alpha, \beta \in T$, 则有

$$\alpha^{p^n} = \alpha,\quad \beta^{p^n} = \beta,$$

随之

$$(\alpha \pm \beta)^{p^n} = \alpha^{p^n} \pm \beta^{p^n} = \alpha \pm \beta,$$
$$(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta,$$
$$(\alpha^{-1})^{p^n} = (\alpha^{p^n})^{-1} = \alpha^{-1}, \quad \alpha \neq 0.$$

即 $\alpha \pm \beta, \alpha\beta, \alpha^{-1}$ 也都是 $f(x)$ 的根,因而都在 T 中.故 T 是子域.

注意到 F 是 $f(x)$ 的分裂域,便得 $F = T$,因而 $|F| = |T| = p^n$. □

上命题说明:元素个数为 p^n 的有限域是存在的,且是 $x^{p^n} - x$ 在 $\mathbb{Z}_p$ 上的分裂域.再注意到分裂域在 $\mathbb{Z}_p$ - 同构的意义下是唯一的,由于 $\mathbb{Z}_p$ 是素域,因而"$\mathbb{Z}_p$ - 同构"和"同构"是一回事,故有

定理 3.3 1) 有限域的元素个数必为形如 p^n 的整数, p 是它的特征;

2) 元素个数为 p^n 的有限域存在且在同构意义下是唯一的.

有限域常称作 Galois 域,元素个数为 p^n 的有限域通常记作 $GF(p^n)$.

下面进一步讨论有限域 F 的结构.首先是它的子域结构.

设 T 是有限域 $F = GF(p^n)$ 的子域.由

$$[F:T]\cdot[T:\mathbb{Z}_p] = [F:\mathbb{Z}_p] = n$$

知 $[T:\mathbb{Z}_p] = m$ 必整除 n. T 是元素个数为 p^m 的有限域.这样 T 是 $x^{p^m} - x$ 在 $\mathbb{Z}_p$ 上的分裂域.注意到 T 是 F 的子域,故

$$T = \{\alpha \in F \mid \alpha^{p^m} - \alpha = 0\}.$$

这样, F 中元素个数为 p^m 的子域 T 有且仅有一个,它由多项式 $x^{p^m} - x$ 在 F 中的一切根组成.

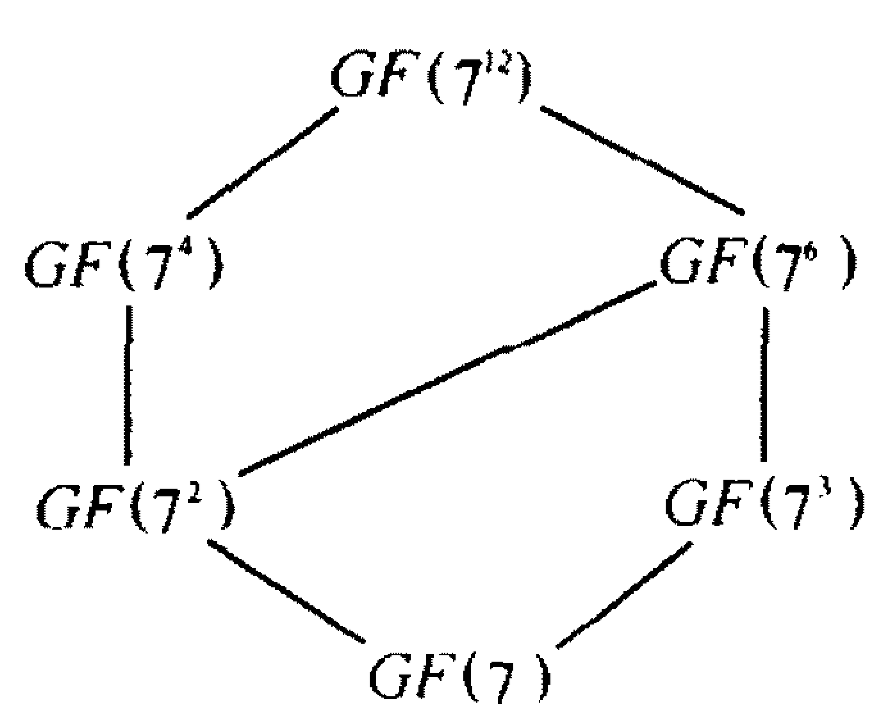
这就证明了下面

命题 3.4 1) 有限域 $GF(p^n)$ 的子域是元素个数为 p^m 的域 $GF(p^m)$,这里 $m \mid n$.

2) 对 n 的任一因子 m,有限域 $GF(p^n)$ 有且仅有一个子域 $GF(p^m)$.

3) 有限域 $GF(p^n)$ 中元素个数为 p^s 的子域包含元素个数为 p^t 的子域当且仅当 $t \mid s$. □

例 $GF(7^{12})$ 的所有子域可排列如下:



其次我们看一下有限域 F 的加群 $(F, +)$ 和乘群 $(F^* = F\setminus\{0\}, \cdot)$ 的结构.这两个有限交换群是结构紧凑的域的有机组成部分,可以想象不是任意交换群都能作为域的乘群的.

有限域 $GF(p^n)$ 是域 $\mathbb{Z}_p$ 上 n 维向量空间,随之它是 n 个一维 $\mathbb{Z}_p$ - 向量空间的直和.这样 $(GF(p^n), +)$ 是 n 个加群 $(\mathbb{Z}_p, +)$ 的直和,即是 n 个 p 阶循环群的直和.这样,有限域 F 的加群,可以说是最简单的有限交换 p - 群.

命题 3.5 有限域 $F = GF(q = p^n)$ 的乘群 $(F^* = F\setminus\{0\}, \cdot)$ 是 $q-1$ 阶循环群.

先证一个

引理 3.6 设 G 是有限交换群,而 m 是 G 中元素的阶的最大者.则对任意 $g \in G$,有 $g^m = e$.

证明提示 先证交换群 G 中,若元素 a 的阶是 s,元素 b 的阶是 t,且 $(s, t) = 1$,则 ab 的阶为 st.由之即得 ab 的阶是 a,b 的阶的最小公倍数.利用这一结果便不难证得上面引理.□

命题 3.5 的证明 有限交换群 F^* 中必有一元素 a,其阶 m 是最大的.当然 $m \leqslant |F^*| = q-1$.由上引理知

$$\text{对任意} \quad x \in F^*, \quad \text{有} \quad x^m = 1. \tag{2}$$

把(2)放在域 F 中来看,它说明 F^* 中 $q-1$ 个元素都是多项式 $x^m - 1$ 的根,这说明 $q-1 \leqslant m$.随之 $m = q-1$,因而 $F^* = (a)$.□

作为上命题的直接推论得

定理 3.7 有限域 $F = GF(p^n)$ 是域 $\mathbb{Z}_p$ 上的单扩域:$F = \mathbb{Z}_p(a)$.□

上定理是说域 $\mathbb{Z}_p$ 上的有限次扩域是单扩域.这是一个很好的定理:把较复杂的有限次扩域归结为单扩域,这也是域 $\mathbb{Z}_p$ 的一个很好的性质.

作为本节结束,我们叙述一个很漂亮的结果.

Wedderburn **定理** 有限除环必是(有限)域.□

练习

1. 若域 F 的元素个数为 p^n,这里 p 为素数,则 F 中每个元有唯一 p 次根.
2. 四元域不能同构于八元域的子域.
3. 找出 $\mathbb{Z}_2[x]$ 的一切三次不可约多项式.
4. 求 $\mathbb{Z}_2$ 上不可约多项式 $f(x)$,使得 $GF(8)$ 是 $f(x)$ 在 $\mathbb{Z}_2$ 上的分裂域.

§4 正规扩域(分裂域续)

为了简单也为了突出本质而略去次要条件,在以下各节中我们只讨论特征 0 的域.这种域有两个性质:它们是无限域,这些域上的不可约多项式没有重根.

分裂域 K/F 的定义是构造性的:它是把一多项式 $f(x)\in F[x]$ 的所有根添加到 F 上所得的扩域 K. 下面将用一个代数性质去刻画它,即给分裂域一个结构性的定义.

定义 4.1　扩域 K/F 称作 F 上正规扩域,如果 K 是 F 上有限次扩域,且若 F 上任一不可约多项式 $p(x)$ 有一个根在 K 中,则 $p(x)$ 的所有根都在 K 中(亦即 $p(x)$ 在 $K[x]$ 中分解成一次因式的乘积).

与代数闭域的概念对比一下是有益的:代数闭域 C 上每一个多项式的全部根都在 C 中,而正规扩域 K/F 是说, F 上一不可约多项式的全部根都在 K 中,如果它有一个根在 K 中.

定义中应特别注意 $p(x)$ 是一个不可约多项式. 对于多项式 $f(x)=g(x)h(x)$, $g(x)$ 的根和 $h(x)$ 的根可以是毫无联系的,因而不能要求 $f(x)$ 的一个根如何,其它的根也如何.

定义 4.2　扩域 K/F 中两个元素 α,β 称为 F – 共轭的,如果它们在 F 上有相同的极小多项式. 或者说 F 上不可约多项式 $p(x)$ 的根是彼此 F – 共轭的.

这当然是共轭复数概念的推广:两复数是共轭的当且仅当它们是同一个二次不可约实多项式的根.

这样,正规扩域 K/F 是说:若 $\alpha\in F$, 则与 α 是 F – 共轭的元素都在 K 中. 或者说扩域 K/F 关于 F – 共轭是封闭的.

定理 4.3　扩域 K/F 是正规扩域当且仅当扩域 K/F 是 F 上的分裂域.

证明　设 K/F 是正规扩域,则由于 K 是 F 上有限次扩域,故 $K=F(\alpha_1,\cdots,\alpha_t)$, t 正整数, α_i 是 F 上代数元,它的 F – 极小多项式记作 $p_i(x)$. F 上不可约多项式 $p_i(x)$ 有一个根 $\alpha_i\in K$, 随之,由正规扩域的定义得 $p_i(x)$ 的所有根都在 K 中. 由之即得 $K=F(\alpha_1,\cdots,\alpha_t)$ 是 $f(x)=p_1(x)\cdots p_t(x)\in F[x]$ 在 F 上的分裂域.

另一方面,设 K 是一 n 次多项式 $f(x)\in F[x]$ 在 F 上的分裂域,即 $K=F(\alpha_1,\cdots,\alpha_n)$, $\alpha_1,\cdots,\alpha_n$ 是 $f(x)$ 的全部根. 又设 F 上不可约多项式 $p(x)$ 有一根 $\beta\in K=F(\alpha_1,\cdots,\alpha_n)$. 类似于用一代数元 α 作单扩张的情形(见命题 2.1)可把 β 写成 $\beta=g(\alpha_1,\cdots,\alpha_n)$, 其中 $g(x_1,\cdots,x_n)$ 是 F 上一个 n 元多项式.

下一步证明将用到根与系数的关系与对称多项式理论. 为此我们先证下面这个

引理　$S_n=\{\Pi_i,1\leqslant i\leqslant n!\}$ 是 $\{1,\cdots,n\}$ 的所有置换组成的 n 元对称群. $F[x_1,\cdots,x_n]$ 是 F 上 n 元多项式环. 今定义群 S_n 对集 $F[x_1,\cdots,x_n]$ 的一个作用,亦即定义 $F[x_1,\cdots,x_n]\times S_n$ 到 $F[x_1,\cdots,x_n]$ 的一个运算如下:对于

$$\Pi=\begin{pmatrix}1 & 2 & \cdots & n\\ \Pi(1) & \Pi(2) & \cdots & \Pi(n)\end{pmatrix}\in S_n,\quad Y(x_1,\cdots,x_n)\in F[x_1,\cdots,x_n],$$

规定

$$Y(x_1,\cdots,x_n)\cdot\Pi=Y(x_{\Pi(1)},\cdots,x_{\Pi(n)}).$$

则有 1) 对任意取定 n 元多项式 Y 和 $\Sigma\in S_n$，有 $\{Y\cdot\Pi_i,1\leqslant i\leqslant n!\}=\{(Y\cdot\Pi_i)\cdot\Sigma,1\leqslant i\leqslant n!\}$；

2) 设 $h(y_1,\cdots,y_{n!})$ 是 $y_i,1\leqslant i\leqslant n!$ 的对称多项式，则 $h(Y\cdot\Pi_1,\cdots,Y\cdot\Pi_{n!})=H(x_1,\cdots,x_n)$ 是 $x_j,1\leqslant j\leqslant n$ 的对称多项式.

证明 1) 直接验证可知

$$(Y\cdot\Pi)\cdot\Sigma=Y\cdot(\Pi\Sigma).$$

另一方面，对于群 S_n 显然有 $S_n\cdot\Sigma=S_n$，即 $\{\Pi_i\Sigma,1\leqslant i\leqslant n!\}=\{\Pi_i,1\leqslant i\leqslant n!\}$，故有

$$\{(Y\cdot\Pi_i)\cdot\Sigma,1\leqslant i\leqslant n!\}=\{Y\cdot\Pi_i,1\leqslant i\leqslant n!\}.$$

2) 证明 $H(x_1,\cdots,x_n)$ 是对称多项式，只需证明

$$\forall\ \Sigma\in S_n,\quad H(x_1,\cdots,x_n)\cdot\Sigma=H(x_1,\cdots,x_n).\qquad(*)$$

首先我们有等式

$$\begin{aligned}H(x_1,\cdots,x_n)\cdot\Sigma&=h(Y(x_1,\cdots,x_n)\cdot\Pi_1,\cdots,Y(x_1,\cdots,x_n)\cdot\Pi_{n!})\cdot\Sigma\\&=h((Y(x_1,\cdots,x_n)\cdot\Pi_1)\cdot\Sigma,\cdots,(Y(x_1,\cdots,x_n)\cdot\Pi_{n!})\cdot\Sigma),\end{aligned}$$

这是因为，对多项式 $H(x_1,\cdots,x_n)$ 的变元 $x_1,\cdots,x_n$ 进行 Σ 置换就等于对其中每一“整体”出现的多项式 $Y(x_1,\cdots,x_n)\cdot\Pi_i$ 的变元 $x_1,\cdots,x_n$ 进行 Σ 置换. 由 1)的结果，以及注意到 $h(y_1,\cdots,y_{n!})$ 是对称多项式便得 $(*)$. □

现在应用这个引理，继续定理的证明.

考察 x 的多项式，

$$\begin{aligned}G(x)=&(x-g(\alpha_1,\cdots,\alpha_n)\cdot\Pi_1)(x-g(\alpha_1,\cdots,\alpha_n)\cdot\Pi_2)\\&\cdots(x-g(\alpha_1,\cdots,\alpha_n)\cdot\Pi_{n!}).\end{aligned}$$

其中 $g(\alpha_1,\cdots,\alpha_n)\cdot\Pi_i$ 是在多项式 $g(x_1,\cdots,x_n)\cdot\Pi_i$ 中令 $x_i=\alpha_i,1\leqslant i\leqslant n$，而得到的 K 中元素. 根据根与系数的关系知 $G(x)$ 的系数都是

$$y_i=g(\alpha_1,\cdots,\alpha_n)\cdot\Pi_i,\quad 1\leqslant i\leqslant n!$$

的初等对称多项式. 根据上面引理知 $G(x)$ 的系数都是 $\alpha_1,\cdots,\alpha_n$ 的对称多项式，因而可通过 $\alpha_1,\cdots,\alpha_n$ 的初等对称多项式，也就是 $f(x)$ 的系数表示. 但 $f(x)$ 的系数都在域 F 中，因而 $G(x)\in F[x]$.

$G(x)$ 有根 $g(\alpha_1,\cdots,\alpha_n)=\beta$（当 π 为恒等置换时，$g(\alpha_1,\cdots,\alpha_n)\pi=g(\alpha_1,\cdots,\alpha_n)$）而 F 上不可约多项式 $p(x)$ 也有根 β. 这样 $(G(x),p(x))=p(x)$，即 $p(x)\mid G(x)$，随之 $p(x)$ 在 K 上分解成一次因式的乘积，即 $p(x)$ 的全部根都在 K 中. □

定理 4.4 F 上有限次扩域 K 是单扩域. 特别地，F 上的分裂域 K 是单

扩域.

证明　$K = F(\alpha_1,\cdots,\alpha_n) = F(\alpha_1)(\alpha_2)\cdots(\alpha_n)$. 只要我们能证 $F(\alpha)(\beta) = F(\theta)$, 即在 F 上添加两个代数元等同于添加某一个代数元,再用一下归纳法就行了.

设 $p(x),q(x)$ 分别是 F 上代数元 α,β 的 F - 极小多项式.

我们希望在 $T = F(\alpha)(\beta)$ 中找到一个元素 θ 使 $\alpha \in F(\theta),\beta \in F(\theta)$. 显然元素 θ 具有形式 $g(\alpha,\beta),g(x,y) \in F[x,y]$. 最简单,也是最先该考虑的,该是设 $\theta = \alpha + c\beta, c \in F$. 这时只要 $\beta \in F(\theta)$, 则也有 $\alpha \in F(\theta)$. 然后设法选 c 以达到我们的目的. 由于关于 α,β 的计算规则由其极小多项式 $p(x),q(x)$ 决定,所以这里一定要充分利用它们.

下面是非常巧妙和关键的一步. 设 $r(x) = p(\alpha + c\beta - cx) \in F(\theta)[x]$, 显然 $r(x)$ 和 $q(x)$ 有公共根 β, 如果我们能够选择 $c \in F$ 使 $r(x)$ 和 $q(x)$ 只有这一个公共根 β, 则由 $r(x) \in F(\theta)[x], q(x) \in F(\theta)[x]$ 便有 $(r(x), q(x)) = x - \beta \in F(\theta)[x]$, 因而得 $\beta \in F(\theta)$, 随之也有 $\alpha \in F(\theta)$.

设 $p(x)$ 的全部根为 $\alpha_1 = \alpha,\alpha_2,\cdots,\alpha_s, q(x)$ 的全部根为 $\beta_1 = \beta,\beta_2,\cdots,\beta_t$, 只要选择 $c \in F$ 满足条件:

$$\alpha + c\beta - c\beta_i \neq \alpha_j, \quad 1 \leqslant i \leqslant t, 2 \leqslant j \leqslant s,$$

即能保证 $r(x)$ 和 $q(x)$ 只有一个公共根 β. 特征 0 的域当然是无限域,这样的 $c \in F$ 是永远存在的. 定理证完. □

建议读者按逻辑顺序整理一下上面证明,并补充好略去的推导.

设 K 是特征为 0 的域 F 上的分裂域,即存在正次数多项式 $f(x) \in F[x]$, 使得在 K 上 $f(x) = a(x-\alpha_1)\cdots(x-\alpha_n)$ 且 $K = F(\alpha_1,\cdots,\alpha_n)$. 不妨设 $\{\alpha_1,\cdots,\alpha_n\}$ 中两两不同根的集合为 $\{\alpha_1,\cdots,\alpha_m\}$, 则 $K = F(\alpha_1,\cdots,\alpha_m)$. 记 $\mathrm{Gal}(K/F)$ 为 K 的全体 F - 自同构关于同构的合成构成的群,我们有:

定理 4.5　设 K 是 F 上关于正次数多项式 $f(x)$ 的分裂域, $f(x)$ 的不同根的集合为 $\{\alpha_1,\cdots,\alpha_m\}$. 任取 $\phi \in \mathrm{Gal}(K/F)$, α 是 $f(x)$ 的一个根,则 $\phi(\alpha)$ 也是 $f(x)$ 的一个根. 这样

$$\Sigma_\phi = \begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_m \\ \phi(\alpha_1) & \phi(\alpha_2) & \cdots & \phi(\alpha_m) \end{pmatrix}$$

是 $M = \{\alpha_1,\alpha_2,\cdots,\alpha_m\}$ 的一个置换.

证明　若 α 是 $f(x)$ 的根. 因 ϕ 保持 F 中元素不变,易证 $\phi(\alpha)$ 也是 $f(x)$ 的根. 由于诸 α_i 彼此不同,而 ϕ 是一一映射,故诸 $\phi(\alpha_i)$ 也彼此不同,即 Σ_ϕ 是 M 的一个置换. □

利用上面结论,我们可以定义群 $\mathrm{Gal}(K/F)$ 到 $\{\alpha_1,\cdots,\alpha_m\}$ 的所有置换作成的群 S_n 的一个映射.

$$\theta: \mathrm{Gal}(K/F) \longrightarrow S_n$$
$$\phi \longmapsto \Sigma_\phi = \begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \phi(\alpha_1) & \phi(\alpha_2) & \cdots & \phi(\alpha_n) \end{pmatrix}.$$

令 $G_f = \{\Sigma_\phi \mid \phi \in \mathrm{Gal}(K/F)\}$，我们有

定理 4.6 记号同上，θ 导出群同构

$$\theta: (\mathrm{Gal}(K/F), \circ) \longrightarrow (G_f, \circ).$$

证明 显然 θ 是满的，易证 θ 是单的．对任意的 $\phi, \psi \in \mathrm{Gal}(K/F)$，有 $\Sigma_\phi \circ \Sigma_\psi = \Sigma_{\phi\circ\psi}$．由此可得 θ 是群同态．因而 θ 是同构．□

定义 4.7 设 K 是 F 上正次数多项式 $f(x)$ 的分裂域，$f(x)$ 的不同根的集合为 $\{\alpha_1, \cdots, \alpha_m\}$，$K = F(\alpha_1, \cdots, \alpha_m)$．称 G_f 为 F 上多项式 $f(x)$ 的根的对称群，也称为 F 上 $f(x)$ 的 Galois 群．并称 $\mathrm{Gal}(K/F)$ 为 F 上分裂域 K 的 Galois 群．

计算一个多项式的 Galois 群有一定的难度．必须对该多项式的根有较好的了解后才有可能．

例 1 计算 $f(x) = (x^2-2)(x^2-3)$ 在 $\mathbb{Q}$ 上的 Galois 群．

解 首先找出 $\mathbb{C}$ 中包含 $\mathbb{Q}$ 以及 $f(x)$ 的不同根 $\alpha_1 = \sqrt{2}, \alpha_2 = -\sqrt{2}, \alpha_3 = \sqrt{3}, \alpha_4 = -\sqrt{3}$ 的最小域 E，容易看到 $E = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}$．这时 $\mathrm{Gal}(E/\mathbb{Q}) = \mathrm{Aut}\, E$．由第一章§2 例 4 知

$$G_f = \left\{ \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \end{pmatrix}, \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \alpha_2 & \alpha_1 & \alpha_3 & \alpha_4 \end{pmatrix}, \right.$$
$$\left. \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \alpha_1 & \alpha_2 & \alpha_4 & \alpha_3 \end{pmatrix}, \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \alpha_2 & \alpha_1 & \alpha_4 & \alpha_3 \end{pmatrix} \right\}.$$

定理 4.8 设 K 是特征 0 的域 F 上的一个分裂域，K 的全体 F－自同构组成的(关于自同构的乘法)群记作 $\mathrm{Gal}(K/F)$．则有

$$[K:F] = |\mathrm{Gal}(K/F)|.$$

证明 由定理 4.4 知 $K = F(\theta)$．设 θ 的 F－最小多项式为 $p(x)$，其次数为 n，并设 $p(x)$ 的全部根，亦即与 θ 成 F－共轭的全部元素为 $\theta_1 = \theta, \theta_2, \cdots, \theta_n$．我们知道 θ_i 彼此不相等且对所有 i，有 $\theta_i \in K$，并且 $[K:F] = n$．

一方面可以证明 $F(\theta) = F(\theta_i)$，且 $F(\theta) \cong F[x]/(p(x)) \cong F(\theta_i)$，故对应

$$\phi_i: K = F(\theta) \longrightarrow K = F(\theta_i)$$
$$f(\theta) \longmapsto f(\theta_i), f(x) \in F[x]$$

是 K 的 F－自同构．

另一方面，若 $\phi \in \mathrm{Gal}(K/F)$，则 $\phi(\theta)$ 也满足 F - 多项式 $p(x)$，$\phi(\theta)$ 等于某个 θ_i，随之 $\phi = \phi_i$.

总起来便是 $\mathrm{Gal}(K/F) = \{\phi_i, 1 \leqslant i \leqslant n\}$，因而 $|\mathrm{Gal}(K/F)| = n = [K:F]$. □

这个重要结果还可以用前一节证明分裂域唯一性的方法去直接证明而不用定理 4.4.

练习

1. K/F 是正规扩域，$K \supseteq E \supseteq F$，则 K/E 也是正规扩域.
2. K/F 是代数扩域，$\{N_i \mid i \in I\}$ 是 K/F 的中间域，且是 F 的正规扩域，求证 $\bigcap\limits_{i \in I} N_i$ 是 F 上正规扩域.
3. K/F 是正规扩域，L/K 是正规扩域，问 L/F 是不是正规扩域？
4. 二次扩域都是正规扩域.

§5 Galois 基本定理

本节中我们介绍著名的 Galois 理论的基本定理. 这是对整个数学发展起重要推动作用的理论之一.

我们仍局限于讨论特征 0 的域的情形. 你完全可以设想我们就是在复数域 $\mathbb{C}$ 中进行的.

设 K/F 是 F 上分裂域. 这里把下面将用到的域论中或群论中的一些结果重温一下：

1) F 上分裂域和 F 上正规扩域是一回事；

2) F 上分裂域 K 是单扩域 $K = F(\theta) = F(\theta_i) = F(\theta_1, \theta_2, \cdots, \theta_n)$，其中 $\{\theta = \theta_1, \theta_2, \cdots, \theta_n\}$ 是 θ 的 F - 最小多项式 $p(x)$ 的全部根；

3) F 上分裂域 $K = F(\theta)$，而 θ 的 F - 最小多项式 $p(x)$ 的次数为 n，则有

$$n = [K:F] = |\mathrm{Gal}(K/F)|.$$

4) $F \subseteq L \subseteq K$，$F, L, K$ 是域，则有 $[K:F] = [K:L][L:F]$.

5) $\{e\} \subseteq H \subseteq G$，$\{e\}$（单位元组成的群），$H, G$ 是有限群，则有

$$|G| = [G:\{e\}] = [G:H][H:\{e\}] = [G:H] \cdot |H|.$$

6) 若 G 是有限群，则对任意 $g \in G$ 有 $gG = Gg = G$.

取定 F 上分裂域 $K = F(\theta)$，设 θ 的一个 F - 极小多项式为 $p(x)$，$G = \mathrm{Gal}(K/F)$. 令

$$\mathbb{K} = \{K/F \text{ 的一切中间域 } L : F \subseteq L \subseteq K\},$$

$$\mathbb{G} = \{G = \mathrm{Gal}(K/F) \text{ 的一切子群 } H : G \supseteq H \supseteq \{e\}\}.$$

以上所用符号在本节中固定下来.

先定义集 $\mathbb{K}$ 到集 $\mathbb{G}$ 的一个对应.

任取 $L \in \mathbb{K}$. 由 $K = F(\theta) \subseteq L(\theta) \subseteq L(\theta_1, \cdots, \theta_n) \subseteq K$ 得 $K = L(\theta) = L(\theta_1, \cdots, \theta_n)$, 因而 K 是多项式 $p(x) \in F[x] \subseteq L[x]$ 在域 L 上的分裂域. 今考虑扩域 L 上分裂域 K 的 Galois 群 $\mathrm{Gal}(K/L)$. 若 $\phi \in \mathrm{Gal}(K/L)$, 即 ϕ 是域 K 的 L - 自同构. ϕ 保持 L 中元素不动, 当然更保持 F 中元素不动, 因而 ϕ 也是 K 的 F - 自同构, 即 $\phi \in \mathrm{Gal}(K/F)$. 随之有 $\mathrm{Gal}(K/L) \subseteq \mathrm{Gal}(K/F) = G$. 这样就得对应

$$\begin{aligned} \mathrm{Gal} : \mathbb{K} &\longrightarrow \mathbb{G} \\ L &\longmapsto \mathrm{Gal}(K/L). \end{aligned}$$

显然 $F \longmapsto \mathrm{Gal}(K/F) = G, K \longmapsto \mathrm{Gal}(K/K) = \{e\}$.

其次定义集 $\mathbb{G}$ 到集 $\mathbb{K}$ 的一个对应.

任取 $H \in \mathbb{G}$. 把 $\alpha \in K$ 在 F - 自同构 ϕ 下的象记作 $\alpha\phi$, 规定

$$\mathrm{Inv}\, H = \{\alpha \in K \mid \forall\, \phi \in H, \alpha\phi = \alpha\}.$$

直接验证可知 $\mathrm{Inv}\, H$ 是 K 的子域且 $F \subseteq \mathrm{Inv}\, H$, 即 $\mathrm{Inv}\, H$ 是中间域, 因而 $\mathrm{Inv}\, H \in \mathbb{K}$. 称 $\mathrm{Inv}\, H$ 为 H 的不变子域(也就是 H - 集 K 的不变元组成的子集). 这样就得对应

$$\begin{aligned} \mathrm{Inv} : \mathbb{G} &\longrightarrow \mathbb{K} \\ H &\longmapsto \mathrm{Inv}\, H. \end{aligned}$$

显然 $\{e\} \longmapsto \mathrm{Inv}\{e\} = K$. 我们还将看到 $G \longmapsto \mathrm{Inv} G = F$.

读者也许已预感到, 下一步想证的该是: 对应 Gal 和对应 Inv 是互逆的, 即想证: $L \in \mathbb{K}, H \in \mathbb{G}$,

$$\mathrm{Inv}(\mathrm{Gal}(K/L)) = L, \tag{1}$$

$$\mathrm{Gal}(K/\mathrm{Inv}\, H) = H. \tag{2}$$

天才的法国青年 Galois 就是利用这两个等式给出了扩域 K/F 的中间域和其(刻画扩域 K/F 的对称性的)Galois 群的子群之间的一一对应. 这就是著名的 Galois 对应. 在数学的其它分支中也出现类似的 Galois 对应, 通过这种对应把不同类型的研究对象(在我们这里是域和群)紧密地联系起来.

证明的关键是下面这个命题.

命题 5.1　设 K 是域 F 上分裂域, $G = \mathrm{Gal}(K/F)$, H 是 G 的一个子群. 而 H 的不变子域 $\mathrm{Inv}\, H = T$. 则有 $[K : T] = |H|$.

证明　令 $H = \{\phi_1, \cdots, \phi_m\}$. 规定群 H 在 $K[x]$ 上的一个右作用, 即定义 $K[x] \times H$ 到 $K[x]$ 的一个运算如下: 设

$$f(x)=b_nx^n+\cdots+b_1x+b_0\in K[x],\ \phi\in H,$$

规定 $$f(x)\cdot\phi=(b_n\phi)x^n+\cdots+(b_1\phi)x+(b_0\phi).$$

注意到 ϕ 是域 K 的自同构，直接演算可知，对 $f(x),g(x)\in K[x],\phi,\phi_i,\phi_j\in H$，

$$f(x)\cdot(\phi_i\phi_j)=(f(x)\cdot\phi_i)\cdot\phi_j,$$

$$(f(x)g(x))\cdot\phi=(f(x)\cdot\phi)(g(x)\cdot\phi).$$

由于正规扩域是单扩域，可设 $K=F(\theta)$. 令

$$h(x)=\prod_{i=1}^{m}(x-\theta\phi_i).$$

对任意 $\phi\in H$ 因为 $H\phi=H$，因而 $\{\theta\phi_i\phi,1\leqslant i\leqslant m\}=\{\theta\phi_i,1\leqslant i\leqslant m\}$. 所以有

$$h(x)\cdot\phi=\Big(\prod_{i=1}^{m}(x-\theta\phi_i)\Big)\phi=\prod_{i=1}^{m}(x-\theta\phi_i\phi)$$

$$=\prod_{i=1}^{m}(x-\theta\phi_i)=h(x).$$

这说明 $h(x)$ 的系数在 $\phi\in H$ 作用下不变，即得 $h(x)\in \mathrm{Inv}\ H[x]=T[x]$. 由于 $T\supseteq F$，由 $K\supseteq T(\theta)\supseteq F(\theta)=K$，得 $K=T(\theta)$. 但 θ 是 T 上 m 次多项式 $h(x)$ 的根，故得

$$[K=T(\theta):T]\leqslant m.$$

另一方面 $\mathrm{Gal}(K/T)\supseteq H$（因为 H 中 ϕ 是 K 的 T-自同构），由定理 4.8 得

$$[K:T]=|\mathrm{Gal}(K/T)|\geqslant|H|=m.$$

合在一起便得 $[K:T]=m=|H|$. □

推论 5.2 符号如上，则 $\mathrm{Inv}\ G=F$.

证明 设 $\mathrm{Inv}\ G=T$. 由上命题得 $[K:T]=n$. 另一方面，有

$$n=[K:F]=[K:T][T:F]=n\cdot[T:F],$$

因而 $[T:F]=1$，即 $T=F$. □

这就是说，对任意分裂域 K/F 都有 $\mathrm{Inv}(\mathrm{Gal}(K/F))=F$. 特别，对于分裂域 K/L 我们有 $\mathrm{Inv}(\mathrm{Gal}(K/L))=L$. 这就是(1).

今证(2). 读者不难证明 $\mathrm{Gal}(K/\mathrm{Inv}\ H)\supseteq H$. 上面命题是说

$$[K:\mathrm{Inv}\ H]=|H|,$$

而另一方面，依定理 4.8，分裂域 $K/\mathrm{Inv}\ H$ 在域 $\mathrm{Inv}\ H$ 上的次数等于其 Galois 群 $\mathrm{Gal}(K/\mathrm{Inv}\ H)$ 的阶，即有

$$[K:\mathrm{Inv}\ H]=|\mathrm{Gal}(K/\mathrm{Inv}\ H)|.$$

合在一起便有

$$|H|=|\mathrm{Gal}(K/\mathrm{Inv}\ H)|,$$

因而有 Gal(K/Inv H) = H，这就是(2).

总起来便得

定理 5.3(Galois 基本定理)　K 是特征 0 域 F 上分裂域.规定

$\mathbb{K}$ = {域 K/F 的一切中间域 $L \mid F \subseteq L \subseteq K$},

$\mathbb{G}$ = {K/L 的 Galois 群 G 的一切子群 $H \mid G \supseteq H \supseteq \{e\}$},

$$\begin{aligned}\mathrm{Gal}: \mathbb{K} &\longrightarrow \mathbb{G}\\ L &\longmapsto \mathrm{Gal}(K/L);\end{aligned}$$

$$\begin{aligned}\mathrm{Inv}: \mathbb{G} &\longrightarrow \mathbb{K}\\ H &\longmapsto \mathrm{Inv}\ H = \{\alpha \in K \mid \forall \phi \in H, \alpha\phi = \alpha\}.\end{aligned}$$

则：

1) Gal, Inv 给出集 $\mathbb{K}$ 和集 $\mathbb{G}$ 间的一一对应且 Gal 和 Inv 互为逆.

2) 若 $L_1 \subseteq L_2, L_1, L_2 \in \mathbb{K}$，则 $\mathrm{Gal}(K/L_1) \supseteq \mathrm{Gal}(K/L_2)$；若 $H_1 \subseteq H_2, H_1, H_2 \in \mathbb{G}$，则 $\mathrm{Inv}\ H_1 \supseteq \mathrm{Inv}\ H_2$. □

结论 2)的证明留给读者.

也许值得再回顾一下这个重要定理的证明.不难得包含关系：

$$\mathrm{Inv}(\mathrm{Gal}(K/L)) \supseteq L, \quad \mathrm{Gal}(K/\mathrm{Inv}\ H) \supseteq H.$$

而能证明这两个包含关系是相等关系全靠两个扩域次数的等式：

$$[K : L] = |\mathrm{Gal}(K/L)|, \quad [K : \mathrm{Inv}\ H] = |H|.$$

下面进一步讨论，当中间域 L 是 F 上正规扩域时，G 的子群 Gal(K/L)) 该有什么更好的性质.将证，它是正规子群.

先证一个命题，它本身再一次说明 Galois 群 Gal(K/F) 刻画着扩域 K/F 的对称性.

命题 5.4　K 是 F 的分裂域. $G = \mathrm{Gal}(K/F) = \{\phi_1$(恒等自同构), $\phi_2, \cdots, \phi_n\}$, $\alpha \in K$，则 $\{\alpha\phi_i, 1 \leqslant i \leqslant n\}$ 恰是 α 的所有 F - 共轭元(可能有相重的).

证明 1　我们知道，$\alpha\phi_i$ 是 α 的 F - 共轭元.今设 β 是 α 的 F - 共轭元，而去证明 β 具有形式 $\alpha\phi_i$. 设

$$\begin{aligned}\psi: F(\alpha) &\longrightarrow F(\beta)\\ a &\longmapsto a\\ \alpha &\longmapsto \beta\\ g(\alpha) &\longmapsto g(\beta), \quad g(x) \in F[x].\end{aligned}$$

由于 α, β 有相同的 F - 极小多项式 $p(x)$，由前知 $\psi: F(\alpha) \longrightarrow F(\beta)$ 是域同构.设 K 是 $F(\alpha)$ 上 $f(x)$ 的分裂域，则 K 也是 $F(\beta)$ 上 $f(x)$ 的分裂域.依命题 2.9，ψ 可开拓成 K 到 K 的一个(自)同构 ϕ 且 $\phi|_{F(\alpha)} = \psi$，随之 $\phi|_F =$

$\psi|_F$ = 域 F 的恒等自同构.这样便得 ϕ 是 K 的 F − 自同构,随之 ϕ 等于某个 ϕ_i : $\phi = \phi_i$. 再由 $\phi|_{F(\alpha)} = \psi$ 便得

$$\alpha\phi_i = \alpha\phi = \alpha\psi = \beta. \square$$

证明 2　只需证 α 的任一 F − 共轭元 $\beta = \alpha\phi_i$, 这次采用命题 5.1 的证明思路,而设

$$g(x) = \prod_{i=1}^{n}(x - \alpha\phi_i),$$

任取 $\phi \in G$, 有

$$g(x)\cdot\phi = \left(\prod_{i=1}^{n}(x - \alpha\phi_i)\right)\phi = \prod_{i=1}^{n}(x - \alpha\phi_i\phi)$$
$$= \prod_{i=1}^{n}(x - \alpha\phi_i) = g(x).$$

第三个等号成立是因为 $G\phi = G$, 因而 $\{\alpha\phi_i\phi, 1 \leqslant i \leqslant n\} = \{\alpha\phi_i, 1 \leqslant i \leqslant n\}$ (带重数). 这样多项式 $g(x) \in K[x]$ 的每一系数在 ϕ 作用下不变,由前面推论 5.2 知这些系数都属于 F, 即 $g(x) \in F[x]$.

$g(x) \in F[x]$ 且以 α 为根,因而必被 α 的 F − 最小多项式 $p(x)$ 整除,即 $g(x) = p(x) \cdot h(x)$. 由 $g(x)$ 的定义可看出 $p(x)$ 的所有根都是形如 $\alpha\phi_i$ 者. $\square$

Galois **基本定理(续)**

3) 若 L 是 F 上正规扩域,则 $\mathrm{Gal}(K/L)$ 是 G 的正规子群;若 H 是 G 的正规子群,则 $\mathrm{Inv}\ H$ 是 F 上正规扩域.

4) 若 L 是 F 上正规扩域,则 $\mathrm{Gal}(L/F) \cong \mathrm{Gal}(K/F)/\mathrm{Gal}(K/L)$.

证明　3) 设 L 是 F 上正规扩域.任取定 $\phi \in G = \mathrm{Gal}(K/F)$, 规定

$$\begin{aligned}\phi' : L &\longrightarrow L\\ \alpha &\longmapsto \alpha\phi.\end{aligned}$$

由上面命题 $\alpha, \alpha\phi$ 是 F − 共轭元,而 $\alpha \in L$ 且 L/F 是正规扩域,故知 $\alpha\phi \in L$, 因而 ϕ' 确是 L 到 L 的对应.易知 ϕ' 还是域 L 的 F − 自同构.这样, $\phi' \in \mathrm{Gal}(L/F)$. 令

$$\begin{aligned}\Sigma : \mathrm{Gal}(K/F) &\longrightarrow \mathrm{Gal}(L/F)\\ \phi &\longmapsto \phi',\end{aligned}$$

注意到 $\phi' = \phi|_L$, 故有

$$\phi'_i\phi'_j = \phi_i|_L \cdot \phi_j|_L = (\phi_i\phi_j)|_L = (\phi_i\phi_j)',$$

即 Σ 是群 $\mathrm{Gal}(K/F)$ 到群 $\mathrm{Gal}(L/F)$ 的一个群同态对应. $\mathrm{Gal}(L/F)$ 的恒等元是域 L 的恒等自同构,故得

$$\begin{aligned}\mathrm{Ker}\Sigma &= \{\phi \in \mathrm{Gal}(K/F) \mid \forall \alpha \in L, \alpha\phi = \alpha\} \\ &= \mathrm{Gal}(K/L).\end{aligned}$$

这样 $\mathrm{Gal}(K/L)$ 是 G 的正规子群. 这就证得 3)中第一句话.

我们还知道 Σ 是一个满的同态对应,这可用两种办法去说明. 其一是,类似命题 5.2 的证明 1,利用命题 2.8 可知:域 L 的任一 F - 自同构都可开拓成域 K 的一个 F - 自同构,随之 Σ 是满的;其二是,由下列等式,对任意正规扩域 E/T, $[E:T] = \mathrm{Gal}(E/T)$, 以及对任意域 $F \subseteq L \subseteq K$ 有

$$[K:L][L:F] = [K:F],$$

随之 $|\mathrm{Gal}(K/L)| \cdot |\mathrm{Gal}(L/F)| = |\mathrm{Gal}(K/F)|$ 即

$$|\mathrm{Gal}(K/F)/\mathrm{Gal}(K/L)| = |\mathrm{Gal}(L/F)|.$$

故得 Σ 是满的.

由 Σ 是群 $\mathrm{Gal}(K/F)$ 到群 $\mathrm{Gal}(L/F)$ 的满同态对应,以及 $\mathrm{Ker}\Sigma = \mathrm{Gal}(K/L)$, 就得 4). 我们把 3)中第二句话的证明留给读者. □

这个基本定理对用根式解代数方程的理论中的重要应用将在 §8 简略地介绍. 在这里,由之立刻可以得到一个有趣结果:分裂域 K/F (因而任意有限次扩域 E/F, 因为 E/F 总可以再扩张成为一个分裂域 K/F)的中间域 L 只有有限多个,这是因为有限群的子群只有有限多个. 一个 $n(\geqslant 2)$ 维 F - 向量空间 K 是有无穷多个 F - 子空间的,上面结果说明,在这无穷多个 F - 子空间中能作成子域的却只有有限多个! 可以说,在代数系统中域是结构最紧致,“要求最高”的一个.

在本节最后,我们再用偏序集和格论的语言陈述一下 Galois 对应.

设 $\{M, \leqslant\}$ 是一个偏序集, $a, b \in M$. 如果 $c \in M$ 具有性质:

1) $a \leqslant c, b \leqslant c$;

2) 若 $x \in M$ 也有 $a \leqslant x, b \leqslant x$, 则必有 $c \leqslant x$,

则我们称 c 为 a, b 的最小上界.

对偶地,如果 $d \in M$ 具有性质:

1) $d \leqslant a, d \leqslant b$;

2) 若 $x \in M$ 也有 $x \leqslant a, x \leqslant b$, 则必有 $x \leqslant d$,

则我们称 d 为 a, b 的最大下界.

当然一个偏序集中的两个元素不一定有最小上界或最大下界. 但另一方面,如果 a, b 的最小上界(最大下界)存在的话,则它必是唯一的(很容易证),常用 $a \vee b$ $(= b \vee a)$ 表示 a, b 的最小上界,用 $a \wedge b$ $(= b \wedge a)$ 表示 a, b 的最大下界.

定义 5.5　若在偏序集 $\{M, \leqslant\}$ 中,对其中任意两元素 a, b, 最小上界 a

$\vee\ b$ 和最大下界 $a \wedge b$ 都存在，则称 $\{M, \leqslant\}$ 为一个格.

和对群和环一样，对偏序集也可以谈论同构或反同构，只不过是把那里的“保持运算”，换成这里的“保持关系”，详细说，就是

定义 5.6 设 $\{M, \leqslant\}$ 和 $\{M', \leqslant\}$ 为两个偏序集. 设

$$\begin{aligned} \phi: M &\longrightarrow M' \\ a &\longmapsto a' \end{aligned}$$

是集 M 到集 M' 上的一一对应.

1) 若 $a \leqslant b$，则 $\phi(a \leqslant \phi(b)$，则称 ϕ 为偏序集 M 到 M' 上的同构对应，而称偏序集 M 同构于偏序集 M'，记作 $M \cong M'$；

2) 若 $a \leqslant b$，则 $\phi(a) \geqslant \phi(b)$，则称 ϕ 为偏序集 M 到 M' 上的反同构对应，而称偏序集 M 反同构于偏序集 M'，记作 $M \cong^{-1} M'$.

命题 5.7 设 $\{M, \leqslant\}$ 和 $\{M', \leqslant\}$ 都是格，

1) 若 $\phi: M \cong M'$，则有 $\phi(a \wedge b) = \phi(a) \wedge \phi(b)$，$\phi(a \vee b) = \phi(a) \vee \phi(b)$；

2) 若 $\phi: M \cong^{-1} M'$，则有 $\phi(a \wedge b) = \phi(a) \vee \phi(b)$，$\phi(a \vee b) = \phi(a) \wedge \phi(b)$.

证明 这里只证，当 $\phi: M \cong^{-1} M'$ 时，必有 $\phi(a \wedge b) = \phi(a) \vee \phi(b)$. 由 $a \wedge b \leqslant a$，$a \wedge b \leqslant b$，知 $\phi(a \wedge b) \geqslant \phi(a)$，$\phi(a \wedge b) \geqslant \phi(b)$. 设 $x \in M'$ 且 $x \geqslant \phi(a)$，$x \geqslant \phi(b)$ 而往证 $x \geqslant \phi(a \wedge b)$. 由于 ϕ 是集 M 到 M' 上的一一对应，故 $x = \phi(y)$，$y \in M$. 注意到 ϕ 是反同构，故由 $\phi(y) = x \geqslant \phi(a)$ 得 $y \leqslant a$，由 $\phi(y) = x \geqslant \phi(b)$ 得 $y \leqslant b$，随之，依 $a \wedge b$ 之定义，知 $y \leqslant a \wedge b$，再依反同构 ϕ 的定义，得 $x = \phi(y) \geqslant \phi(a \wedge b)$. 总起来，这就证明了 $\phi(a \wedge b)$ 是 $\phi(a)$，$\phi(b)$ 的最小上界，即 $\phi(a \wedge b) = \phi(a) \vee \phi(b)$.
□

现在回到扩域 K/F 及其 Galois 群 $\mathrm{Gal}(K/F)$.

易见集 $\mathbb{G} = \{\mathrm{Gal}(K/F)$ 的一切子群$\}$ 关于子群的包含关系 $\subseteq$ 作成一个偏序集，$\{\mathbb{G}, \subseteq\}$ 还是一个格，这是因为，若 $H \in \mathbb{G}$，$J \in \mathbb{G}$，则 $\mathrm{Gal}(K/F)$ 的子群 H, J 生成的子群 $H \cup J$ 就是 H, J 的最小上界，而子群 H, J 之交 $H \cap J$（它也是子群）就是 H, J 的最大下界.

同样集 $\mathbb{K} = \{$扩域 K/F 的一切中间域$\}$ 关于中间域的包含关系 $\subseteq$ 作成一个偏序集. 读者不难仿上证明，$\{\mathbb{K}, \subseteq\}$ 也是一个格.

至此，我们已清楚地看到，Galois 对应（Gal 和 Inv）恰是格 $\{\mathbb{K}, \subseteq\}$ 和格 $\{\mathbb{G}, \subseteq\}$ 之间的反同构. 格 $\{\mathbb{K}, \subseteq\}$ 给出扩域 K/F 的所有中间域之间的关系图，格 $\{\mathbb{G}, \subseteq\}$ 给出群 $\mathrm{Gal}(K/F)$ 的所有子群的关系图，而 Galois 对应是说，只要倒置过来看，这两个关系图是一样的.

练习

1. 设 F 是一个域，$K = F(\alpha)$，$\alpha^n = 1$，其中 n 是使等式 $\alpha^n = 1$ 成立的最小正整数，证明：

1) $K = F(\alpha)$ 是分裂域.

2) K/F 的 Galois 群是 Abel 群.

2. 设域 K 为域 F 的分裂域，M, L 为中间域，证明：

$$\mathrm{Gal}(K/LM) = \mathrm{Gal}(K/L) \cap \mathrm{Gal}(K/M).$$

§6 一个例子

现在来考察一个具体例子，也是回顾和总结一下有关 Galois 理论的基本内容.

设 K 是多项式 $f(x) = (x^2 + x + 1)(x^3 - 2)$ 在有理数域 $\mathbb{Q}$ 上的分裂域. $x^2 + x + 1$ 的根为 $\omega = \frac{1}{2}(-1 + i\sqrt{3}), \omega^2 = \frac{1}{2}(-1 - i\sqrt{3})$ $(\omega^3 = 1)$，而 $x^3 - 2$ 的根为 $\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$. 这样依分裂域的定义，

$$K = \mathbb{Q}(\omega, \omega^2, \sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2) = \mathbb{Q}(\omega, \sqrt[3]{2}).$$

容易看到 $K = \mathbb{Q}(\omega)(\sqrt[3]{2})$，$\omega$ 的一个 $\mathbb{Q}$ - 极小多项式是 $x^2 + x + 1$，$\sqrt[3]{2}$ 的一个 $\mathbb{Q}(\omega)$ - 极小多项式(和它的 $\mathbb{Q}$ - 极小多项式一样)是 $x^3 - 2$.

今按定理 4.8 的证明思路来找出 Galois 群 $\mathrm{Gal}(K/\mathbb{Q})$，即域 K 的所有 $\mathbb{Q}$ - 自同构.

域 $\mathbb{Q}(\omega)$ 是 $\mathbb{Q}$ 的单扩张，其 $\mathbb{Q}$ - 自同构就是 $\mathbb{Q}$ 中元保持不动而把 ω 映到它的 $\mathbb{Q}$ - 共轭元上. ω 的 $\mathbb{Q}$ - 共轭元共有两个：ω 和 ω^2，这样 $\mathbb{Q}(\omega)$ 的 $\mathbb{Q}$ - 自同构也有两个：

$$\begin{aligned} \psi_1 : \mathbb{Q}(\omega) &\longrightarrow \mathbb{Q}(\omega) \\ a &\longmapsto a, a \in \mathbb{Q} \\ \omega &\longmapsto \omega; \end{aligned} \qquad \begin{aligned} \psi_2 : \mathbb{Q}(\omega) &\longrightarrow \mathbb{Q}(\omega^2) = \mathbb{Q}(\omega) \\ a &\longmapsto a, a \in \mathbb{Q} \\ \omega &\longmapsto \omega^2. \end{aligned}$$

域 $K = \mathbb{Q}(\omega)(\sqrt[3]{2})$ 是 $\mathbb{Q}(\omega)$ 的单扩张，$\mathbb{Q}(\omega)$ 的每一($\mathbb{Q}$ -)自同构 ψ 都可开拓成 K 的($\mathbb{Q}$ -)自同态，办法是：将 $\mathbb{Q}(\omega)$ 的元素按 ψ 去对应而把 $\sqrt[3]{2}$ 映到它的 $\mathbb{Q}(\omega)$ - 共轭元上. $\sqrt[3]{2}$ 的 $\mathbb{Q}[\omega]$ - 共轭元共有三个：$\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$，这样每个 ψ 可开拓成 K 的三个自同构，共得 $K = \mathbb{Q}(\omega)(\sqrt[3]{2})$ 的六个 $\mathbb{Q}$ - 自同构如下页的表.

也可直接证明，也可由等式 $|\mathrm{Gal}(K/\mathbb{Q})| = [K : \mathbb{Q}] = [K : \mathbb{Q}[\omega]] \cdot [\mathbb{Q}[\omega] : \mathbb{Q}] = 3 \cdot 2 = 6$ 得知，$G = \{\phi_1, \cdots, \phi_6\}$ 就是 $\mathrm{Gal}(K/\mathbb{Q})$，当然也就是

$$\phi_1 : \mathbb{Q}(\omega) \to \mathbb{Q}(\omega)$$

$$\begin{array}{lll}
\phi_1 : K \to K & \phi_2 : K \to K & \phi_3 : K \to K \\
\quad a \mapsto a, a \in \mathbb{Q} & \quad a \mapsto a, a \in \mathbb{Q} & \quad a \mapsto a, a \in \mathbb{Q} \\
\quad \omega \mapsto \omega & \quad \omega \mapsto \omega & \quad \omega \mapsto \omega \\
\quad \sqrt[3]{2} \mapsto \sqrt[3]{2} & \quad \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega & \quad \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega^2
\end{array}$$

$$\phi_2 : \mathbb{Q}(\omega) \to \mathbb{Q}(\omega)$$

$$\begin{array}{lll}
\phi_4 : K \to K & \phi_5 : K \to K & \phi_6 : K \to K \\
\quad a \mapsto a, a \in \mathbb{Q} & \quad a \mapsto a, a \in \mathbb{Q} & \quad a \mapsto a, a \in \mathbb{Q} \\
\quad \omega \mapsto \omega^2 & \quad \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega & \quad \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega \\
\quad \sqrt[3]{2} \mapsto \sqrt[3]{2} & \quad \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega & \quad \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega^2
\end{array}$$

$\mathbb{Q}$ 上多项式 $f(x) = (x^2 + x + 1)(x^3 - 2)$ 的 Galois 群．若想把 ϕ_i 通过 $f(x)$ 的根的置换来表示，只要看一下 $f(x)$ 的 5 个根（$r_1 = \sqrt[3]{2}, r_2 = \sqrt[3]{2}\omega, r_3 = \sqrt[3]{2}\omega^2, r_4 = \omega, r_5 = \omega^2$）在 ϕ_i 下的象便行了．写出来便是（用 i 代替 r_i）：

$$\phi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = (1),$$

$$\phi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} = (1\ \ 2\ \ 3),$$

$$\phi_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix} = (1\ \ 3\ \ 2),$$

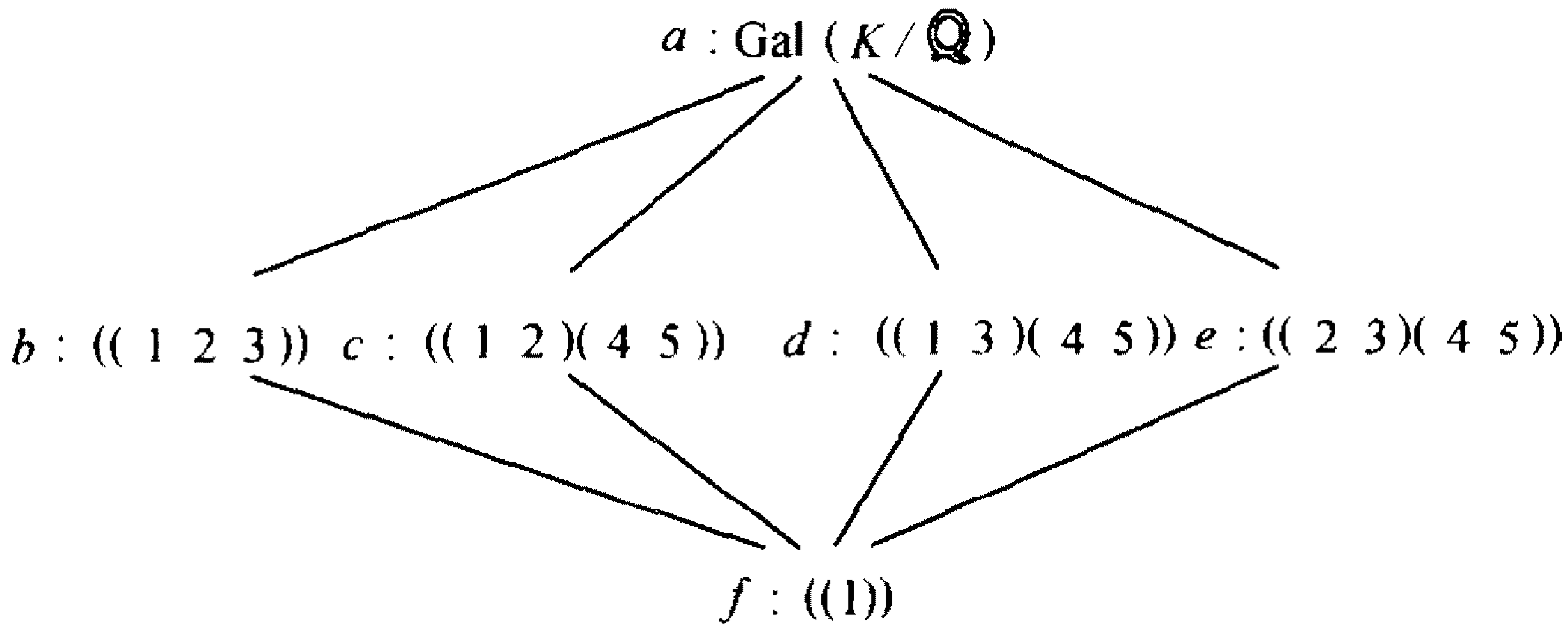
$$\phi_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 5 & 4 \end{pmatrix} = (2\ \ 3)(4\ \ 5),$$

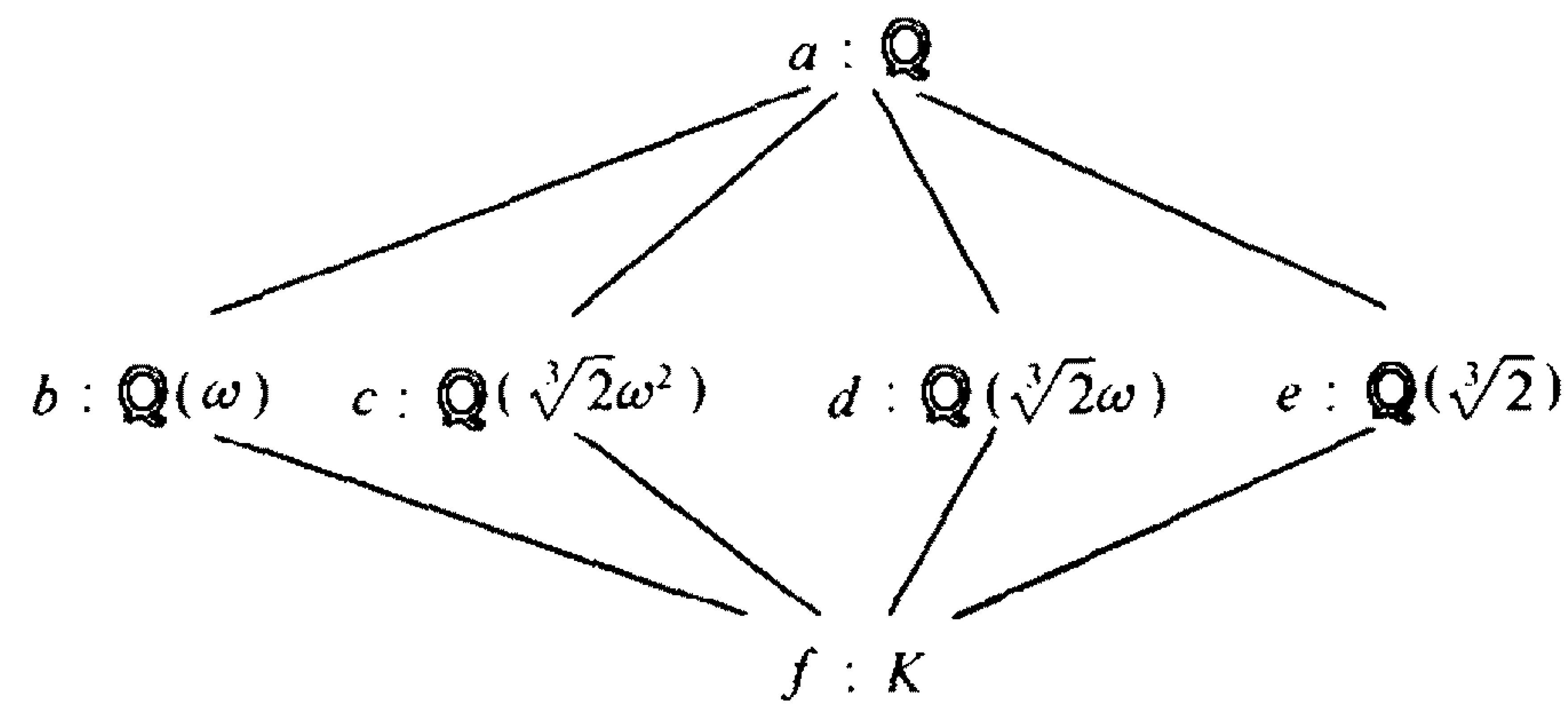
$$\phi_5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix} = (1\ \ 2)(4\ \ 5),$$

$$\phi_6 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix} = (1\ \ 3)(4\ \ 5).$$

在这里再一次的看到，反映根的对称性的这些置换，$\mathbb{Q}$ - 共轭的根间是可互换的，而不是 $\mathbb{Q}$ - 共轭的根间是不相往来的．容易看出 $\mathrm{Gal}(K\mathbb{Q}) \cong S_3$（把 ϕ_i 这些置换局限在 $\{1,2,3\}$ 上，便得到 $\mathrm{Gal}(K/\mathbb{Q})$ 到 $\{1,2,3\}$ 的对称群 S_3 上的同构对应）．

找出一个有限群的所有子群，较之找出扩域的所有中间域要容易得多．所以可先找 $\mathrm{Gal}(K/\mathbb{Q})$ 的子群表，然后用对应 Inv 而得 $K/\mathbb{Q}$ 的中间域表：





上两表编号相同的子群和中间域是在 Galois 对应下互相对应的，如编号都是 d 的子群 $((1\quad 3)(4\quad 5))$ 和中间域 $\mathbb{Q}(\sqrt[3]{2}\omega)$ 有关系：

$$\mathrm{Inv}((1\quad 3)(4\quad 5)) = \mathbb{Q}(\sqrt[3]{2}\omega),$$

$$\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}\omega)/\mathbb{Q}) = ((1\quad 3)(4\quad 5)) = (\phi_6).$$

在上子群表中编号为 b 者是 G 的唯一的真正规子群，这样由 Galois 基本定理知编号为 b 的中间域 $\mathbb{Q}(\omega)$ 是唯一的 $\mathbb{Q}$ 上(不同于 $\mathbb{Q}$ 和 K)的正规扩域，且有

$$\mathrm{Gal}(\mathbb{Q}[\omega]/\mathbb{Q}) \cong S_3/((1\quad 2\quad 3)).$$

最后，由分裂域都是单扩域的证明知，对我们这个具体例子有

$$K = \mathbb{Q}(\omega,\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}+\omega),$$

即 K 是在 $\mathbb{Q}$ 上添加一个数 $\sqrt[3]{2}+\omega$ 所得到的扩域. 也许有兴趣看一下 $\sqrt[3]{2}+\omega$ 的 $\mathbb{Q}$-极小多项式 $p(x)$，它是 6 次($\mathbb{Q}$ 上)不可约多项式. 不难得到 $p(x)$ 的所有根，也就是 $\sqrt[3]{2}+\omega$ 的所有 $\mathbb{Q}$-共轭数，为此只要用 $\mathrm{Gal}(K/\mathbb{Q})$ 中元去作用它即得，即

$$(\sqrt[3]{2}+\omega)\phi_1 = \sqrt[3]{2}+\omega, \qquad (\sqrt[3]{2}+\omega)\phi_2 = \sqrt[3]{2}\omega+\omega,$$

$$(\sqrt[3]{2}+\omega)\phi_3 = \sqrt[3]{2}\omega^2+\omega, \qquad (\sqrt[3]{2}+\omega)\phi_4 = \sqrt[3]{2}+\omega^2,$$

$$(\sqrt[3]{2}+\omega)\phi_5 = \sqrt[3]{2}\omega+\omega^2, \qquad (\sqrt[3]{2}+\omega)\phi_6 = \sqrt[3]{2}\omega^2+\omega^2.$$

利用根与系数的关系可以得到，例如 $p(x)$ 的 x^5 的系数是这六个根之和冠以负号，这就是 3. 有兴趣的读者还可计算出 $p(x)$ 的其它系数.

下面从另一角度再看一下上面的例子. 设 K 是多项式 $g(x) = x^3 - 2$ 在

有理数域 $\mathbb{Q}$ 上的分裂域. x^3-2 的根为 $\sqrt[3]{2},\sqrt[3]{2}\omega,\sqrt[3]{2}\omega^2$, 这样

$$K=\mathbb{Q}(\sqrt[3]{2},\sqrt[3]{2}\omega,\sqrt[3]{2}\omega^2)=\mathbb{Q}(\sqrt[3]{2},\sqrt[3]{2}\omega)=\mathbb{Q}(\sqrt[3]{2})(\sqrt[3]{2}\omega).$$

显然这个域 K 就是上例中的域 K. $\sqrt[3]{2}$ 的 $\mathbb{Q}$ - 极小多项式是 x^3-2, 而 $\sqrt[3]{2}\omega$ 的 $\mathbb{Q}(\sqrt[3]{2})$ - 极小多项式是 $g(x)=x^2+\sqrt[3]{2}x+\sqrt[3]{2}$. $\sqrt[3]{2}$ 的 $\mathbb{Q}$ - 共轭数是 $\sqrt[3]{2},\sqrt[3]{2}\omega,\sqrt[3]{2}\omega^2$, $\sqrt[3]{2}\omega$ 的 $\mathbb{Q}(\sqrt[3]{2})$ - 共轭数是 $\sqrt[3]{2}\omega,\sqrt[3]{2}\omega^2$. 还是按命题的证明思路去找 $\mathrm{Gal}(K/\mathbb{Q})$, 先看 $\mathbb{Q}(\sqrt[3]{2})$ 的 $\mathbb{Q}$ - 同构, 然后再把这些 $\mathbb{Q}$ - 同构开拓成 $K=\mathbb{Q}(\sqrt[3]{2})(\sqrt[3]{2}\omega)$ 的 $\mathbb{Q}$ - 自同构. 由于 $\sqrt[3]{2}$ 有三个 $\mathbb{Q}$ - 共轭数, 故 $\mathbb{Q}(\sqrt[3]{2})$ 有三个 $\mathbb{Q}$ - 同构:

$$\begin{aligned}\psi_1:\mathbb{Q}(\sqrt[3]{2})&\longrightarrow\mathbb{Q}(\sqrt[3]{2})\\ a&\longmapsto a,\ a\in\mathbb{Q}\\ \sqrt[3]{2}&\longmapsto\sqrt[3]{2};\end{aligned}\qquad\begin{aligned}\psi_2:\mathbb{Q}(\sqrt[3]{2})&\longrightarrow\mathbb{Q}(\sqrt[3]{2}\omega)\\ a&\longmapsto a,\ a\in\mathbb{Q}\\ \sqrt[3]{2};&\longmapsto\sqrt[3]{2}\omega;\end{aligned}$$

$$\begin{aligned}\psi_3:\mathbb{Q}(\sqrt[3]{2})&\longrightarrow\mathbb{Q}(\sqrt[3]{2}\omega^2)\\ a&\longmapsto a,\ a\in\mathbb{Q}\\ \sqrt[3]{2}&\longmapsto\sqrt[3]{2}\omega^2.\end{aligned}$$

由于 $\sqrt[3]{2}\omega$ 有二个 $\mathbb{Q}(\sqrt[3]{2})$ - 共轭数, 故 ψ_1 可开拓成 K 的两个 $\mathbb{Q}$ - 自同构. 写出来便是

$$\psi_1:\mathbb{Q}(\sqrt[3]{2})\to\mathbb{Q}(\sqrt[3]{2})$$

$$\begin{aligned}\phi_1:K&\longrightarrow K\\ a&\longmapsto a,\ a\in\mathbb{Q}\\ \sqrt[3]{2}&\longmapsto\sqrt[3]{2}\\ \sqrt[3]{2}\omega&\longmapsto\sqrt[3]{2}\omega\end{aligned}\qquad\begin{aligned}\phi_4:K&\longrightarrow K\\ a&\longmapsto a,\ a\in\mathbb{Q}\\ \sqrt[3]{2}&\longmapsto\sqrt[3]{2}\\ \sqrt[3]{2}\omega&\longmapsto\sqrt[3]{2}\omega^2\end{aligned}$$

今考察 ψ_2 的情况. $\psi_2:\mathbb{Q}(\sqrt[3]{2})\longrightarrow\mathbb{Q}(\sqrt[3]{2}\omega)$. $K=\mathbb{Q}(\sqrt[3]{2})(\sqrt[3]{2}\omega)$. 由 ψ_2 得环同构(仍记作 ψ_2)

$$\begin{aligned}\psi_2:\quad \mathbb{Q}(\sqrt[3]{2})[x]&\longrightarrow\mathbb{Q}(\sqrt[3]{2}\omega)[x]\\ x^n+b_{n-1}x^{n-1}+\cdots+b_0&\longmapsto x^n+(\psi_2b_{n-1})x^{n-1}+\cdots+(\psi_2b_0)\\ g(x)=x^2+\sqrt[3]{2}x+\sqrt[3]{4}&\longmapsto x^2+\sqrt[3]{2}\omega x+\sqrt[3]{4}\omega^2=\bar{g}(x),\end{aligned}$$

$\bar{g}(x)$ 的两个根是 $\sqrt[3]{2}$ 和 $\sqrt[3]{2}\omega^2$. 让 $g(x)$ 的根 $\sqrt[3]{2}\omega$ 去对应 $\bar{g}(x)$ 的每一个根便把 ψ_2 开拓到 $K=\mathbb{Q}(\sqrt[3]{2})(\sqrt[3]{2}\omega)$ 到 $K=\mathbb{Q}(\sqrt[3]{2}\omega)(\sqrt[3]{2})$ (或 $K=\mathbb{Q}(\sqrt[3]{2}\omega)(\sqrt[3]{2}\omega^2)$)的 $\mathbb{Q}$ - 自同构, 写出来便是:

ψ_3 和 ψ_2 的情况类似, 写出结果便是

$$\varphi_2 : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\sqrt[3]{2}\omega)$$

$$\begin{array}{rcl} \phi_5 : K & \to & K \\ a & \mapsto & a, a \in \mathbb{Q} \\ \sqrt[3]{2} & \mapsto & \sqrt[3]{2}\omega \\ \sqrt[3]{2}\omega & \mapsto & \sqrt[3]{2} \end{array} \qquad \begin{array}{rcl} \phi_2 : K & \to & K \\ a & \mapsto & a, a \in \mathbb{Q} \\ \sqrt[3]{2} & \mapsto & \sqrt[3]{2}\omega \\ \sqrt[3]{2}\omega & \mapsto & \sqrt[3]{2}\omega^2 \end{array}$$

$$\varphi_3 : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\sqrt[3]{2}\omega^2)$$

$$\begin{array}{rcl} \phi_3 : K & \to & K \\ a & \mapsto & a, a \in \mathbb{Q} \\ \sqrt[3]{2} & \mapsto & \sqrt[3]{2}\omega^2 \\ \sqrt[3]{2}\omega & \mapsto & \sqrt[3]{2} \end{array} \qquad \begin{array}{rcl} \phi_6 : K & \to & K \\ a & \mapsto & a, a \in \mathbb{Q} \\ \sqrt[3]{2} & \mapsto & \sqrt[3]{2}\omega^2 \\ \sqrt[3]{2}\omega & \mapsto & \sqrt[3]{2}\omega \end{array}$$

这样 $\mathrm{Gal}(K/\mathbb{Q}) = \{\phi_1, \cdots, \phi_6\}$. 当然 $\mathrm{Gal}(K/\mathbb{Q})$ 也是多项式 $x^2 - 3$ 的 Galois 群,把其元素写成 $x^2 - 3$ 的三个根的置换就是(设 $\alpha_1 = \sqrt[3]{2}, \alpha_2 = \sqrt[3]{2}\omega, \alpha_3 = \sqrt[3]{2}\omega^2$, 并用 i 代替 α_i):

$$\phi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = (1), \quad \phi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1 \quad 2 \quad 3),$$

$$\phi_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1 \quad 3 \quad 2), \quad \phi_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2 \quad 3),$$

$$\phi_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1 \quad 2), \quad \phi_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1 \quad 3).$$

和上面一样,还可以先找出 $\mathrm{Gal}(K/\mathbb{Q})$ 的子群表,再按对应 Inv 找出扩域 $K/\mathbb{Q}$ 的中间域表,这一工作留给读者. 当然结果是和上例中完全一样的.

练习

1. $K = \mathbb{Q}(\sqrt{-3}, \sqrt[3]{2})$ 是 $\mathbb{Q}$ 的分裂域.

   1) 写出 $\mathrm{Gal}(K/\mathbb{Q})$;

   2) 找出 $\mathrm{Gal}(K/\mathbb{Q})$ 的所有子群以及它们对应的中间域.

2. $K = \mathbb{Q}(\sqrt[4]{3}, i)$ 是 $\mathbb{Q}$ 的分裂域.

   1) 写出 $\mathrm{Gal}(K/\mathbb{Q})$;

   2) 找出 $\mathrm{Gal}(K/\mathbb{Q})$ 的所有子群以及它们对应的中间域,并指出哪些是正规子群以及对应的正规扩域.

§7　尺规作图不能问题

我们都熟悉初等几何的尺规作图，即用无刻度直尺和圆规作出平面几何图形．如果一个作图问题，如平分已知角，可以用尺规作出，当然它就是一个尺规作图可能问题．如果一个作图问题，如三等分一个已知角，你长久作不出来，或者二千年来没有人能作出，它是一个难题，但远不能说是一个尺规作图不能问题．要在数学上肯定一个作图问题是尺规作图不能问题，就必须否定一切可能性．一个好的方式是应用反证法而去证明：若该问题能用尺规作出，则必导出矛盾．数学中的矛盾当然是指在某一公理体系下的矛盾．因而若想谈论尺规作图不能问题，必须把含直观因素的尺规作图概念进行数学刻画，即公理化．下面就来作这件事．

尺规作图的出发点是已知一些初等几何图形（诸如三角形、圆等），一些线段，一些点，而求作也是一些初等几何图形，线段，点等．但无论是初等几何图形，还是线段等都可以归结为点．这样尺规作图问题就可概括成：已知平面上的一些点，要求用尺规作出另一些点．

在取定某线段为单位长引入直角坐标系后，直观的平面上的点就可用实数对 (a,b) 代替，其中 $a(b)$ 是 x － 轴上（ y － 轴上）某有向线段的度量，这样尺规作图问题就可说成：已知一些实数，如 1（单位长），$a_1,\cdots,a_n$，要求用尺规作出另一些实数 $\alpha_1,\cdots,\alpha_m$．

我们知道用尺规可以作出：

1）若干线段之和；

2）两线段之差；

3）已知三线段 a,b,c 可作出线段 x 使 $a:b=c:x$；

4）已知二线段 a,b 可作出线段 y 使 $a:y=y:b$．

把这些功能用这些线段的度量去表达，就是如果已知正实数 $1,|a_1|,\cdots,|a_n|$，我们可以用尺规作出它们的和，差，积，商和开平方．在此基础上，再赋予它们以适当的 $\pm$ 符号，便知：已知一些实数 $1,a_1,\cdots,a_n$，可用尺规作出域 $\mathbb{Q}(a_1,\cdots,a_n)$ 中的实数以及对任意 $b\in\mathbb{Q}(a_1,\cdots,a_n)$，$b>0$，可作出 $\mathbb{Q}(a_1,\cdots,a_n)(\sqrt{b})$ 中的实数．更一般地，若能从 $1,a_1,\cdots,a_n$ 出发用尺规作出实数组成的域 F 中的数，则对任意 $b\in F,b>0$，可用尺规作出 $F(\sqrt{b})$ 中的实数．

定义 7.1　设 $F\subseteq K$，F,K 是实数域 $\mathbb{R}$ 的子域（简称之为实域）．如果 $K=F(\sqrt{b_1})(\sqrt{b_2})\cdots(\sqrt{b_m})$，其中所有 $b_i>0,b_1\in F,b_i\in$

$F(\sqrt{b_1})\cdots(\sqrt{b_{i-1}})$, $i \geqslant 2$, 则称 K 为 F 的 Pythagoras(毕达哥拉斯)扩域,简称毕氏扩域.

这样,以上的讨论说明:由已知实数 $1, a_1, \cdots, a_n$ 出发,可用尺规作出 $F = \mathbb{Q}(1, a_1, \cdots, a_n)$ 上的任意毕氏扩域中的数.

下一个问题是:我们是否相信这些 F 上毕氏扩域中的数就是用尺规由 $1, a_1, \cdots, a_n$ 出发可作出的所有数?为此我们回顾一下尺规作图时通常采用的步骤:

1. 在平面上的某个范围内,或在已作出的直线或圆上,任选一点;
2. 过两已知点作一直线;
3. 过已知点用已知半径作一圆;
4. 作出两已知直线的交点;
5. 作出一已知直线和一已知圆的交点;
6. 作出两已知圆的交点.

应该说这些就是尺规作图时为得到新点所有能采取的步骤.现在分析一下,这些步骤能提供一些什么样的新点(=新实数).设实域 E 是已知的.这时的已知直线和已知圆在我们的坐标系下就相当 x, y 的一次方程 $ax + by + c = 0$ 和二次方程 $x^2 + y^2 + ax + by + c = 0$,而其系数在已知实域 E 中,当采用第 4,5,6 步骤时,所得新的坐标(实数)必在域 E 的毕氏扩域中.注意到 F 的毕氏扩域的毕氏扩域仍是 F 上的毕氏扩域,因而第 4,5,6 步骤能提供的新数走不出已知域 $F = \mathbb{Q}(1, a_1, \cdots, a_n)$ 的毕氏扩域的范围.

关于步骤 1 的任选一点.这当然不允许你选择特殊点,例如你不能通过任选"一已知角的三等分线上的一点",以说明你会用尺规三等分角.因而在抽象化这一作图步骤时,把它明确为:在平面上可任选一坐标为有理数的点(有理点);在已知图形(直线或圆)上可选两有理点连线与之相交的那些点.这样,步骤 1 能提供给我们新数仍是出发域 F 上的毕氏扩域中的数.

作图步骤 2,3,则是为获得新点作的准备,或是最终作出所求图形.

总起来说,如果你承认我们在初等几何尺规作图中能作的是(这是没有问题的)且仅是(这似乎应慎重一些)上述六个步骤有限次的反复使用,则由已知数 $1, a_1, \cdots, a_n$ 出发能用尺规作出的数将是且仅是实域 $\mathbb{Q}(1, a_1, \cdots, a_n)$ 的毕氏扩域中的数.

一方面,经过上述分析,上述对尺规作图这个刻画是完全可接受的.另一方面,实域的毕氏扩域是严格的数学概念,而尺规作图则是在实践中有共识的直观概念,在数学概念与非数学的直观概念之间无法运用数学推理去证明它们的等价,我们只能把这种刻画看成是尺规作图的一种数学模型或尺规作图的一种公理化。

初等几何尺规作图的数学模型:由已知数 $1,a_1,\cdots,a_n$ 出发能用尺规作出的数是且仅是实域 $F=\mathbb{Q}(1,a_1,\cdots,a_n)$ 的毕氏扩域中的数.

当然这是尺规作图的一种数学模型,就是说它也许还有另外的更令人满意的数学模型,尽管目前尚没有被提出来.

该强调一下的是,当讨论尺规作图"能问题"时,我们不需要这个尺规作图的公理化,因为 F 的毕氏扩域中的数,我们会用尺规作出,能作出来,它当然是个"能问题".但是当谈论尺规作图"不能问题"时,就需要这个尺规作图的公理化作为我们的共同出发点,是须臾不能离开的.

命题 7.2　K 是域 F 的扩域且 $[K:F]=$ 奇数,则 K 必不含在 F 的毕氏扩域中.

证明　设 $F\subseteq K\subseteq E$,而 E 是 F 的毕氏扩域.依定义知 $[E:F]=2^n$.再由 $[E:F]=[E:K][K:F]$ 而 $[K:F]$ 是奇数,便得矛盾.□

下面看一下古希腊时代就开始讨论的三大几何作图问题.

例 1　三等分角问题:设 α 是已知角,试三等分之,即求角 θ 使 $3\theta=\alpha$.由三角公式,有

$$\cos\alpha=\cos3\theta=4\cos^3\theta-3\cos\theta.$$

这样所求的 $\cos\theta$ 是三次多项式 $4x^3-3x-\cos\alpha$ 的根.如果这个三次多项式(例如当 $\alpha=60^\circ$ 而 $\cos\alpha=\dfrac{1}{2}$ 时)是域 $F=\mathbb{Q}(\cos\alpha)$ 上的不可约多项式,则 $F(\cos\theta)$ 是 F 上三次扩域,因而依上命题,$F(\cos\theta)$ 不可能含在 F 的一个毕氏扩域中,随之 $\cos\theta$ 不能用尺规作出,即三等分角是尺规作图不能问题.

例 2　立方倍积问题:已知一边长为 a 的立方体,求作一立方体其体积是它的 2 倍.设所求立方体的边长为 b,则易见 b 是多项式 x^3-2a^3 的根.如果这个三次多项式(例如当 $a=1$ 时)是域 $F=\mathbb{Q}(a)$ 上的不可约多项式,则 $F(b)$ 是 F 上三次扩域,随之 $F(b)$ 不可能含在 F 的一个毕氏扩域中,即所求 b 不能用尺规作出.即立方倍积问题是尺规作图不能问题.

例 3　化圆为方问题:将已知半径为 a 的圆化成一个等积的正方形.设所求正方形的边长为 b,则 b 满足多项式 $x^2-\pi a^2$,即 $b=a\sqrt{\pi}$.这样求 b 就等于求 π.这时已知域是 $F=\mathbb{Q}(a)$,而当 $F(\pi)$(例如当 $a=1$)是 F 上 ∞ 次扩域(π 是超越数)时,显然它不能包含于 F 的毕氏扩域中,因而化圆为方问题也是尺规作图不能问题.

值得回顾一下的是,我们完整而顺利地解决了尺规作图不能问题,用到的只是域论中一个最基本而简单的事实:$F\subseteq E\subseteq K$,F,E,K 都是域,则有 $[K:F]=[K:E][E:F]$.另一方面,再一次看到,把几何问题化归为代数问题不但是有效的,而且是漂亮的.

§8 用根式解代数方程问题

用根式解代数方程问题是一个把经典代数引到近世代数(即抽象代数)的有划时代意义的问题.在这里回顾一下历史是有益的.由于篇幅限制将略去证明.

经典代数是以解代数方程问题为中心展开的.大约公元前 2000 年,古巴比伦人就已经知道类似于我们大家熟悉的配方法解一元二次方程.在中学我们就学过

$$x^2 + bx + c = 0$$

的解是 $x = \dfrac{-b \pm \sqrt{b^2 - 4c}}{2}$.

关于一元三次方程,S. del. Ferro (1465 – 1526)和 N. Fontan linebreak(即 Tartaglia) (1499 – 1557)给出了解法,而对于一元四次方程,L. Ferrari (1522 – 1565)给出了一个解法,都收入在 1545 年出版的、G. Cardano (1501 – 1576)的代数巨著 Ars Magna(《大术》)中.他们的解法,也就是最古老的解法,用我们现在习惯的方式可表达如下:

一般一元三次方程

$$x^3 + ax^2 + bx + c = 0 \tag{1}$$

在用 $x - \dfrac{a}{3}$ 代替 x 后可化成形如:

$$x^3 + mx = n \tag{2}$$

的方程,因而只需求(2)的解.利用恒等式

$$(u - v)^3 + 3uv(u - v) = u^3 - v^3,$$

把它与(2)比较而得 $x = u - v, 3uv = m, u^3 - v^3 = n$.

由后面的两个关于 u, v 的方程,可解得

$$u = \sqrt[3]{(n/2) + \sqrt{(n/2)^2 + (m/3)^3}},$$

$$v = \sqrt[3]{-(n/2) + \sqrt{(n/2)^2 + (m/3)^3}}.$$

从而得方程(2)的解的公式

$$x = \sqrt[3]{(n/2) + \sqrt{(n/2)^2 + (m/3)^3}} - \sqrt[3]{-(n/2) + \sqrt{(n/2)^2 + (m/3)^3}}.$$

这就是被称作 Cardana – Tartaglia 公式.

一般一元四次方程在作一个适当的变量替换后可化成

$$x^4 + px^2 + qx + r = 0 \tag{3}$$

的形式，利用配方法，可把(3)写成

$$(x^2+p)^2 = px^2 - qx + p^2 - r,$$

因而引入参数 y 后有

$$(x^2+px+y)^2 = (p+2y)x^2 - qx + (p^2 - r + 2py + y^2). \qquad (4)$$

下一步是选择 y 使得(4)的右侧是一个完全平方. 为此只需选 y 适合方程

$$4(p+2y)(p^2 - r + 2py + y^2) - q^2 = 0,$$

这是一个关于 y 的三次方程，从而用前面方法可解得 y. 利用这个 y 值，求(4)的解 x 也就是求(3)解 x，就变成开平方和再解一个一元二次方程的问题了.

由此可见在 16 世纪中叶已有了二、三、四次方程的公式解. 虽然我们没有直接写出四次方程解的公式，但不难看出，所有这些方程的解都可以通过原方程的系数经过四则运算和开方运算表示出，即二、三、四次方程有根式解.

面对这样重要，漂亮的结果，数学界自然要迎接下一个挑战：找出五次方程的根式解. 1545 年以来近 300 年的努力，这中间特别应提到 Lagrange, Gauss, P. Ruffini(1765－1822), N. H. Abel(1802－1829)等人的名字，直到 1830 年才由天才的法国数学家 Galois 完全解决了：存在五次方程它不能用根式解. 对 Galois 以前的工作我们只想提到下面的几个.

Lagrange 分析了当时所有已知的解方程的方法，并指出可用一个统一的方法去代替这些不同的解法. 他的想法是：设 n 次方程 $x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = 0$ 的 n 个根为 $\alpha_1, \cdots, \alpha_n$，任取这些根 α_i 的一个有理函数

$$r(\alpha_1, \cdots, \alpha_n) = \frac{f(\alpha_1, \cdots, \alpha_n)}{g(\alpha_1, \cdots, \alpha_n)},$$

其中 $f(\alpha_1, \cdots, \alpha_n), g(\alpha_1, \cdots, \alpha_n)$ 是 $\alpha_1, \cdots, \alpha_n$ 的有理系数多项式.

考虑根的置换 $\pi = \begin{pmatrix} \alpha_1 & \cdots & \alpha_n \\ \alpha_{\pi(1)} & \cdots & \alpha_{\pi(n)} \end{pmatrix}$ 或 $\pi = \begin{pmatrix} 1 & \cdots & n \\ \pi(1) & \cdots & \pi(n) \end{pmatrix}$，其中 $\pi(1)\pi(2)\cdots\pi(n)$ 是 $1,2,\cdots,n$ 的一个排列，并规定 π 对有理式 r 的作用如下：

$$r\pi = \frac{f(\alpha_{\pi(1)}, \cdots, \alpha_{\pi(n)})}{g(\alpha_{\pi(1)}, \cdots, \alpha_{\pi(n)})}.$$

根据对称多项式的基本定理以及根与系数的关系，Lagrange 证明一个命题：如果诸根 α_i 的某一有理函数 r 在所有 n 次置换 π 作用下只取 m 个不同的值，则 r 必适合一个 m 次多项式 $P(x)$，其系数是原方程的系数(即 $a_1, \cdots, a_n$)的有理函数. 根据这个命题，如果能找到合适的有理函数 r 而使 $m < n$，就可将要解的方程的次数降低. 在讨论过程中 Lagrange 引入置换，置换的乘法，置换群的概念. 所有这些，我们今日都可以在 Galois 理论中看到它们的影子.

Lagrange 的学生意大利人 P. Ruffini 证明了一般 n 次方程，当 $n \geqslant 5$ 时不

能用根式解. 然而他是在"方程的解的根式表达式中,每一根号下的式子都是方程的诸根以及单位根的有理函数"这一假设下证明的. 后来 Abel 证明了上面这一假设是成立的,并再一次独立地得到了 Ruffini 的证明,至此就完整地证明一般 n 次方程,当 $n \geqslant 5$ 时不能用根式解.

我们熟悉的方程论中的基本定理,后被称作"代数基本定理"是 Gauss 第一次证明的,他对方程论的另一个重要工作是证明分圆方程式 $x^m - 1 = 0$ 的根式解. 这里用"根式解"的意义是:设 ξ_m 是 m 次本原单位根,则由 De Moivre 公式有

$$\xi_m = \cos\frac{2\pi}{m} + i\sin\frac{2\pi}{m} = a_m + b_m i.$$

Gauss 证明了,必有扩域链 σ

$$\begin{aligned}\mathbb{Q} = F_1 \subset F_1(\sqrt[n_1]{d_1}) = F_2 \subset F_2(\sqrt[n_2]{d_2}) = F_3 \subset \cdots \\ \subset F_s(\sqrt[n_s]{d_s}) = F_{s+1} \subset \mathbb{R},\end{aligned}$$

其中 $d_i \in F_i$, F_i 是实数域 $\mathbb{R}$ 的子域,而 $a_m, b_m \in F_{s+1}$. 特别该提一下的,当 $n = 17$, 这些自然数 n_i 都等于 2,因而实数 a_{17}, b_{17} 可用圆规直尺作出,也就是说,正十七边形是可以用圆规直尺作出的.

以上简单回顾了 Galois 以前的工作.

下面我们利用前面详细讨论过的 Galois 基本定理来介绍完整、完美地解决五次方程不能用根式解的问题,但由于篇幅限制,仍将略去证明.

首先给出根式解的定义. 它是我们心目中根式解的数学刻画.

定义 8.1 设 F 是特征 0 的域, $f(x) \in F[x]$ 是一个 n 次多项式,设 H 是 F 上 $f(x)$ 的分裂域,若存在 F 上的扩域链

$$F = F_1 \subseteq F_1(\theta_1) = F_2 \subseteq F_2(\theta_2) = F_3 \subseteq \cdots \subseteq F_s(\theta_s) = K, \quad (5)$$

其中 $\theta_i^{n_i} = d_i \in F_i$, n_i 是自然数, $1 \leqslant i \leqslant s$, 且 $H \subseteq K$, 则称 $f(x)$ 可用根式解. 并称 K 为 F 的根式扩域.

该说一下的是,按此定义,则显然直接可得分圆多项式 $x^m - 1$ 是可用根式解的,这是和 Gauss 证明的定理: $x^m - 1$ 可用根式解中所用"根式解"的意义是不同的.

F 的根式扩域 K 一般不是 F 的正规扩域. 然而可以证明(略去):若 K 是 F 的根式扩域,则 F 的含 K 的最小正规扩域 $\overline{K}$ (若 $K = F(\alpha)$ 而 α 在 F 上的最小多项式是 $g(x)$, 则 $\overline{K}$ 就是 $g(x)$ 在 F 上的分裂域)也是 F 的根式扩域. 这样,不失一般性,在下面我们认定上面定义(5)中的根式扩域 K 是 F 的正规扩域.

在根式扩域链(5)中, F_{i+1} 一般不是 F_i 的正规扩域,但如果我们假设域

F，对所有正整数 n，包含所有 n 次单位根，这时 F_{i+1} 将是 F_i 上 $x^{n_i}-d_i$ 的分裂域，因而是 F_i 上的正规扩域. 下面为了简单，将认定 F 含所有 n 次单位根，$\forall\ n\in\mathbb{Z}^+$.

这样，(5)中 K 是 F 的正规扩域，F_{i+1} 是 F_i 的正规扩域，$\forall\ i$.

下一步来应用 Galois 基本定理，把域论语言刻画的(5)翻译成群论语言. 为此我们需要下面命题(略去证明).

命题 8.2　设域 F 含所有 n 次单位根而 L 是域 F 上 x^n-d 的分裂域，则 $\mathrm{Gal}(L/F)$ 是交换群. □

对 F 的正规扩域——根式扩域 K 应用 Galois 基本定理，则有下面的对应：$G=\mathrm{Gal}(K/F)$，

$$\begin{array}{ccccccccc}
F=F_1 & \subseteq & F_1(\theta_1)=F_2 & \subseteq\cdots\subseteq & F_i(\theta_i)=F_{i+1} & \subseteq\cdots\subseteq & F_s(\theta_s)=K \\
\updownarrow & & \updownarrow & & \updownarrow & & \updownarrow \\
\mathrm{Gal}(K/F_1) & \supseteq & \mathrm{Gal}(K/F_2) & \supseteq\cdots\supseteq & \mathrm{Gal}(K/F_{i+1}) & \supseteq\cdots\supseteq & \mathrm{Gal}(K/K) \\
\| & & \| & & \| & & \| \\
G=G_1 & \triangleright & G_2 & \triangleright\cdots\triangleright & G_{i+1} & \triangleright\cdots\triangleright & G_s=\{e\}
\end{array}$$

其中 $G_1\triangleright G_2$(也写成 $G_2\triangleleft G_1$)表示：G_2 是群 G_1 的正规子群.

注意到 F_{i+1}是 F_i 的正规扩域，对 F_i 上正规扩域 K：

$$F_i\subseteq F_{i+1}\subseteq K.$$

应用 Galois 基本定理，则知 G_{i+1}是 G_i 的正规子群，且有

$$G_i/G_{i+1}=\mathrm{Gal}(K/F_i)/\mathrm{Gal}(K/F_{i+1})\cong\mathrm{Gal}(F_{i+1}/F_i).$$

再据上面命题，$\mathrm{Gal}(F_{i+1}/F_i)$，因而与之同构的 G_i/G_{i+1}是交换群. 这样，F 的根式扩域——正规扩域 K 的 $\mathrm{Gal}(K/F)$是具有特殊性质的群，这些群值得给一个反映其出身背景的专用名称.

定义 8.3　称一个有限群 G 为可解群，如果 G 中有一子群链：

$$\{e\}=G_s\triangleleft G_{g-1}\triangleleft\cdots\triangleleft\ G_{i+1}\triangleleft G_i\triangleleft\cdots\triangleleft\ G_1=G,$$

其中 G_{i+1}是 G_i 的正规子群，且商群 G_i/G_{i+1}是交换群.

我们略去证明而给出下面

命题 8.4　可解群的子群和商群仍是可解群. □

这样，上面的讨论说明，当 F 含所有 n 次单位根，$\forall\ n$，则 F 的根式扩域——正规扩域 K 的 Galois 群 $\mathrm{Gal}(K/F)$是可解群.

现在来看 $f(x)\in F[x]$ 的分裂域 H 而假定 $f(x)$ 可用根式解. 这时依定义及上面的讨论，有 F 的根式扩域——正规扩域 K 使得 $F\subseteq H\subseteq K$. 注意到 H 是 F 的正规扩域，故据 Galois 基本定理有

$$\mathrm{Gal}(H/F)\cong\mathrm{Gal}(K/F)/\mathrm{Gal}(K/H),$$

即 $\mathrm{Gal}(H/F)$ 是可解群 $\mathrm{Gal}(K/F)$ 的商群，依上面命题，它也是可解群.

总结一下就是:在 F 含所有 n 次单位根, $\forall\ n$, 的假定下, $f(x)\in F[x]$ 可用根式解,则其分裂域 H 的 Galois 群 $\mathrm{Gal}(H/F)$ 是可解群.

实际上,我们有下面更一般更完善的结果(略去证明).

定理 8.5　F 是特征 0 的域. $f(x)\in F[x]$ 可用根式解当且仅当 $f(x)$ 的(分裂域 H 的)Galois 群 $\mathrm{Gal}(H/F)$ 是可解群.

下面来看五次方程不能用根式解问题.为此只需找出五次多项式 $f(x)$,其 Galois 群不是可解群.

数域 E 上一般五次方程是指

$$f(x)\equiv x^5+a_1x^4+a_2x^3+a_3x^2+a_4x+a_5=0,$$

其中 a_1,a_2,a_3,a_4,a_5 是多元多项式环 $E[a_1,\cdots,a_5]$ 中的无关不定元.这样 $f(x)$ 是分式域 $E(a_1,\cdots,a_5)=F$ 上的多项式.可以证明:此 $f(x)$ 在 F 上的 Galois 群同构于对称群 S_5. 另一方面交代群 A_5 是单群且非交换,故 A_5 不是可解群,随之 S_5 不是可解群.这就说明数域上一般五次方程不能用根式解.

另一方面,可以证明:有理数域 $\mathbb{Q}$ 上五次多项式 $x^5+20x+16$ 的 Galois 群也是 S_5, 因而五次方程 $x^5+20x+16=0$ 是不能用根式解的.

有兴趣的读者请参看相应的参考书.

§9　有限域的一个应用——编码

现代通讯技术以及电子计算机技术总是离不开编码理论的.在数字通讯中总是先把要传送的信息转换成数字信息.工程上最易实现的是二元数字信息,也就是由符号 0,1 组成的长为 n 的符号串.用我们习惯的代数语言表述,这就是有限域 $GF(2)$上的一个 n 维向量.例如下表中把空格,英文字母等信息转换成长为 5 的二元数字信息.在现代通讯技术下,很容易把二元数字信息从甲地经信道传到乙地.这样只要把信息源 I 转换成二元数字信息集 $M(I)$ 就可以传送了.但信道是常被干扰的,也就是说,乙地真正收到的并不一定是甲地发出的.如何加工改造 $M(I)$,使得乙地能根据已收到的,可能包含错误的符号串在一定意义下判断出甲地的真正意图,这正是我们数学应该解决的问题.

信息	二元数字信息
空格	00000
a	00001
b	00010
c	00011
⋮	⋮

撇开通讯理论的细节而突出数学实质.让我们在上述背景下讨论下面这个数学问题:

取定正整数 n.设 $F=GF(2)$是二元域而用 F^n 表示由所有 n 维向量 $\boldsymbol{a}=(a_1,\cdots,a_n)$,$a_i\in F$,$i=1,\cdots,n$,组成的 F 上 n 维向量空间,称 F^n 的一个非空子集 M 为一个码,称 M 中的元素为码 M 的码字(在没有混淆时,常简称为码字),称 F^n 中的元素为字.我们的问题是:

C1. 如何简单易行地构造一个码 M?

C2. 如何简单造一个码 M,使得我们能有效地判断,任意字 $\boldsymbol{x}$(设想为乙地收到者)是否是 M 的码字,即是否有 $\boldsymbol{x}\in M$(检错码)?

C3. 如何构造一个码 M,使得我们可以判断,一个给定的字 $\boldsymbol{a}$(乙地收到者)是来源于 M 中的哪个码字 $\boldsymbol{a}'$? 或者说这个给定字 $\boldsymbol{a}$“最接近”,“最像”M 中的哪个码字 $\boldsymbol{a}'$,而使我们可把 $\boldsymbol{a}$ 译为码字 $\boldsymbol{a}'$(纠错码).

两个字的分量相同的愈多当然愈接近.例如,若

$$\boldsymbol{x}=(011010),$$
$$\boldsymbol{y}_1=(011011),$$
$$\boldsymbol{y}_2=(111110),$$

字 $\boldsymbol{x}$ 和 $\boldsymbol{y}_1$ 只在第 6 分量上不一样而 $\boldsymbol{x}$ 和 $\boldsymbol{y}_2$ 在第 1 和第 4 两个分量上都不一样,自然地认定字 x 更接近字 $\boldsymbol{y}_1$.如果码 M 就是由 $\boldsymbol{y}_1,\boldsymbol{y}_2$ 组成,那么当乙地收到的是字 $\boldsymbol{x}$ 时,乙地应该认为甲地发来的是码字 $\boldsymbol{y}_1$ 而不是 $\boldsymbol{y}_2$.而其根据则是:数字正确地通过信道的概率比发生错误的概率要大一些.在此背景下我们给出下面

定义 9.1 在 F^n 中任取两个字 $\boldsymbol{x},\boldsymbol{y}$,并设

$$\boldsymbol{x}=(x_1,x_2,\cdots,x_n),$$
$$\boldsymbol{y}=(y_1,y_2,\cdots,y_n).$$

规定 $\rho(\boldsymbol{x},\boldsymbol{y})$为 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 中对应分量不相等的个数,即满足 $x_i\neq y_i$ 的 i 的个数,称之为 $\boldsymbol{x}$ 到 $\boldsymbol{y}$ 的 Hamming 距离,常简称为距离.

这样 Hamming 距离是非负整数.容易证明下面

定理 9.2 F^n 中的 Hamming 距离 $\rho(\boldsymbol{x},\boldsymbol{y})$有下列性质:

1. $\rho(\boldsymbol{x},\boldsymbol{y})=0$ 当且仅当 $\boldsymbol{x}=\boldsymbol{y}$;

2. $\rho(\boldsymbol{x},\boldsymbol{y})=\rho(\boldsymbol{y},\boldsymbol{x})$;

3.(三角形不等式)对任意 $\boldsymbol{x},\boldsymbol{y},\boldsymbol{z}\in F^n$,有

$$\rho(\boldsymbol{x},\boldsymbol{y})+\rho(\boldsymbol{y},\boldsymbol{z})\geqslant\rho(\boldsymbol{x},\boldsymbol{z}). \qquad \square$$

上定理说明:Hamming 距离具有通常距离的所有性质.

设 M 是 F^n 的一个码,$\boldsymbol{a}\in F^n$,规定

$$\rho(\boldsymbol{a},M)=\min\{\rho(\boldsymbol{a},\boldsymbol{x}),\boldsymbol{x}\in M\},$$

$$\rho(M,M)=\min\{\rho(\boldsymbol{x},\boldsymbol{y}),\boldsymbol{x}\in M,\boldsymbol{y}\in M\text{ 且 }\boldsymbol{x}\neq\boldsymbol{y}\}$$

并称 $\rho(M,M)$ 为码 M 的最小距离,而 $\rho(\boldsymbol{a},M)$ 为字 $\boldsymbol{a}$ 到码 M 的距离.

问题 C3 中的“最接近”,“最像”的数学刻画就是下面的

最大似然译码原理:$M\subseteq F^n$ 是一个码而 $\boldsymbol{a}\in F^n$(设想为乙地收到者).若存在唯一的 $\boldsymbol{a}'\in M$ 满足条件 $\rho(\boldsymbol{a},\boldsymbol{a}')=\rho(\boldsymbol{a},M)$,则我们将认定 $\boldsymbol{a}$ 就是码字 $\boldsymbol{a}'$(即 $\boldsymbol{a}'$ 就是甲地发出者)的误传,并将字 $\boldsymbol{a}$ 译为码字 $\boldsymbol{a}'$.

此原理是说,应把 $\boldsymbol{a}$ 解释为与之距离最小的那个码字 $\boldsymbol{a}'$.原理中的唯一性是重要的:如果有 $\boldsymbol{b},\boldsymbol{c}\in M$,并且

$$\rho(\boldsymbol{a},\boldsymbol{b})=\rho(\boldsymbol{a},M)=\rho(\boldsymbol{a},\boldsymbol{c}),$$

这时我们就不知道该把 $\boldsymbol{a}$ 解释为码字 $\boldsymbol{b}$ 还是码字 $\boldsymbol{c}$ 了.

定义 9.3 一个码 M 称作可纠正 t 个差错的纠错码,如果对满足 $\rho(\boldsymbol{a},M)\leqslant t$(其意义是假设一个码字通过信道后最多在 t 个分量位置上出错)的字 $\boldsymbol{a}$,总有唯一的 $\boldsymbol{a}'\in M$ 使 $\rho(\boldsymbol{a},\boldsymbol{a}')=\rho(\boldsymbol{a},M)$.这时就可依最大似然译码原理把 $\boldsymbol{a}$ 译为码字 $\boldsymbol{a}'$ 了.

容易证明(利用 Hamming 距离的性质)下面

定理 9.4 若码 M 的最小距离 $\rho(M,M)=2t+1$,t 是正整数,则 M 是可纠正 t 个差错的纠错码. $\square$

这样,解决问题 C3 的一个办法就是构造最小距离尽可能大的码.

下面我们依次来解决上述三个问题.

首先是问题 C1.把 F^n 的一个杂乱无章的子集 M 当作码是不足取的:只能靠列举给出它且很难研究其性质.选具有某种结构的子集 M 当作码显然是个好主意.首先想到的该是具有代数结构的码.

定义 9.5 F^n 的一个 k 维子空间 L 称作线性码,或更详细一些,(n,k) 线性码,此时 L 中的任一码字都是 F^n 中 k 个线性无关向量的线性组合.

给定一个 (n,k) 线性码 L 是一件轻而易举的事:只要在 F^n 中选出 k 个线性无关的向量 $\boldsymbol{g}_1,\boldsymbol{g}_2,\cdots,\boldsymbol{g}_k$ 来就行了.设 $k\times n$ 矩阵

$$G=\begin{pmatrix}\boldsymbol{g}_1\\ \vdots\\ \boldsymbol{g}_k\end{pmatrix}=\begin{pmatrix}g_{11} & g_{12} & \cdots & g_{1n}\\ g_{21} & g_{22} & \cdots & g_{2n}\\ \cdots & \cdots & \cdots & \cdots\\ g_{k1} & g_{k2} & \cdots & g_{kn}\end{pmatrix}, \qquad (1)$$

则 L 中任一码字可唯一地表成$(\alpha_1,\alpha_2,\cdots,\alpha_k)\cdot G,\alpha_i\in F$,且这种形式的向量都是 L 中的码字.称矩阵 G 为码 L 的生成矩阵.

对这个(n,k)线性码 L 我们来讨论问题 C2.这也就是判断一个 n 维向量 $\boldsymbol{a}$ 是否属于子空间 L,或是否能表成 $\boldsymbol{g}_1,\cdots,\boldsymbol{g}_k$ 的线性组合.由线性代数(当然是指有限域上而不是数域上的线性代数)知,这是不难解决的.下面也许是最方便的一种方法.令齐次线性方程组

$$G\cdot\boldsymbol{x}^T=\begin{pmatrix}g_{11}&\cdots&g_{1n}\\\cdots&\cdots&\cdots\\g_{k1}&\cdots&g_{kn}\end{pmatrix}\begin{pmatrix}x_1\\\vdots\\x_n\end{pmatrix}\begin{pmatrix}0\\\vdots\\0\end{pmatrix}$$

(其中 $\boldsymbol{x}=(x_1,\cdots,x_n)$,$\boldsymbol{x}^T$ 是 $\boldsymbol{x}$ 的转置向量)的解空间为 L^*,它是 F^n 的一个 $n-k$ 维子空间.取 L^* 的一个基 $\boldsymbol{h}_i=(h_{i1},h_{i2},\cdots,h_{in})$,$i=1,\cdots,n-k$,而设 $(n-k)\times n$ 矩阵

$$H=\begin{pmatrix}\boldsymbol{h}_1\\\vdots\\\boldsymbol{h}_{n-k}\end{pmatrix}=\begin{pmatrix}h_{11}&h_{12}&\cdots&h_{1n}\\h_{21}&h_{22}&\cdots&h_{2n}\\\cdots&\cdots&\cdots&\cdots\\h_{n-k,1}&h_{n-k,2}&\cdots&h_{n-k,n}\end{pmatrix}.\tag{2}$$

由线性代数知,F^n 的向量 $\boldsymbol{a}\in L$ 当且仅当 $H\cdot\boldsymbol{a}^T=0$,这里 $\boldsymbol{0}$ 是零向量.这样,对任意字 $\boldsymbol{a}\in F^n$,只要计算一下 $H\cdot\boldsymbol{a}^T$,根据它是不是零向量就可判断 $\boldsymbol{a}$ 是否是 L 中的码字,对(n,k)线性码就顺利地解决了问题 C2.称矩阵 H 为码 L 的校验矩阵.

当然,一个线性码 L 的生成矩阵 G 和校验矩阵 H 不是唯一的.我们每次只是取定一个 G 和一个 H.

现在来讨论问题 C3.从上面的讨论知,这里最重要的事是计算线性码 L 的最小距离 $\rho(L,L)$.

设 $\boldsymbol{a}\in F^n$,规定 $\boldsymbol{a}$ 的重 $W(\boldsymbol{a})$为 $\boldsymbol{a}$ 中非 0 分量的个数.这样,$W(\boldsymbol{a})$取值非负整数而零向量 $\boldsymbol{0}$ 的重 $W(\boldsymbol{0})=0$.易知

$$\rho(\boldsymbol{x},\boldsymbol{y})=W(\boldsymbol{x}-\boldsymbol{y}).$$

这样,注意到线性码 L 是子空间,因而对减法是封闭的,便有

$$\begin{aligned}\rho(L,L)&=\min\{\rho(\boldsymbol{x},\boldsymbol{y})=W(\boldsymbol{x}-\boldsymbol{y}),\boldsymbol{x}\in L,\boldsymbol{y}\in L,\boldsymbol{x}\neq\boldsymbol{y}\}\\&=\min\{W(\boldsymbol{a}),\boldsymbol{a}\in L\text{ 且 }\boldsymbol{a}\neq\boldsymbol{0}\},\end{aligned}$$

也就是说计算线性码 L 的最小距离只需数一数 L 中非零向量的非零分量的个数就可以了.

设(n,k)线性码 L 的生成矩阵 G 如(1)而校验矩阵 H 如(2).我们已知 $\boldsymbol{a}\in L$ 当且仅当 $H\cdot\boldsymbol{a}^T=\boldsymbol{0}$.若用 $\boldsymbol{\alpha}_1,\cdots,\boldsymbol{\alpha}_n$ 表示矩阵 H 的 n 个列向量而 $\boldsymbol{a}=$

$(a_1,\cdots,a_n)$,则 $H\cdot \boldsymbol{a}^T=\mathbf{0}$.的意思就是

$$a_1\boldsymbol{\alpha}_1+a_2\boldsymbol{\alpha}_2+\cdots+a_n\boldsymbol{\alpha}_n=\mathbf{0}.$$

如果列向量 $\boldsymbol{\alpha}_1,\cdots\boldsymbol{\alpha}_n$ 中任意 s 个都线性无关,则 a_i 中非零个数就不能小于或等于 s,即 $W(\boldsymbol{a})>s$.若又知列向量 $\boldsymbol{\alpha}_1,\cdots,\boldsymbol{\alpha}_n$ 中确存在 $s+1$ 个线性相关向量,比如说是前 $s+1$ 个,则有

$$1\cdot\boldsymbol{\alpha}_1+1\cdot\boldsymbol{\alpha}_2+\cdots+1\cdot\boldsymbol{\alpha}_{s+1}+0\cdot\boldsymbol{\alpha}_{s+2}+\cdots+0\cdot\boldsymbol{\alpha}_n=\mathbf{0},$$

而这说明

$$\boldsymbol{b}=(\underbrace{1,1,\cdots,1}_{s+1\text{个}},0,\cdots,0)\in L,$$

即 L 中存在码字 $\boldsymbol{b}$ 有 $W(\boldsymbol{b})=s+1$.总起来,在上面约定的条件下,有 $\rho(L,L)=s+1$.

在上面我们是选定生成矩阵 G 以确定一个线性码 L.其实我们也完全可以先选定校验矩阵 H,而依 $\boldsymbol{a}\in L$ 当且仅当 $H\cdot\boldsymbol{a}^T=\mathbf{0}$ 来确定一个线性码 L.

这样,选定(2)中的矩阵 H,满足条件:a) H 的 $n-k$ 个行向量线性无关;b) H 的 n 个列向量中任意 s 个都线性无关,而有 $s+1$ 个列向量线性相关(即 H 的列秩为 s),则以 H 为校验矩阵的 (n,k) 线性码 L 之最小距离为 $s+1$,因而它是可纠 t(如果 $s=2t$)个差错的纠错码.

关于编码问题的一般讨论就到此.下面来看一个例子.

例 取 F^4 中所有 $2^4-1=15$ 个非零向量,以它们为列向量按某个顺序排列起来便得一个 4×15 矩阵.如果取自然顺序,即是正整数 i 的 2 进制表示放在第 i 列处,则得

$$H_1=\begin{pmatrix}0&0&0&0&0&0&0&1&1&1&1&1&1&1&1\\0&0&0&1&1&1&1&0&0&0&0&1&1&1&1\\0&1&1&0&0&1&1&0&0&1&1&0&0&1&1\\1&0&1&0&1&0&1&0&1&0&1&0&1&0&1\end{pmatrix}.$$

显然 H_1 的秩为 4,因而 H 的 4 个 15 维行向量是线性无关的,即满足上面条件 a). H_1 的 15 个列向量中任意两个都不相同,注意到域 $F=GF(2)$,便知它们是线性无关的.另一方面 H_1 的前三个列向量是线性相关的,总起来便有 H 满足上面条件 b),且 $s=2$,随之得以 H_1 为校验矩阵的 $(15,11)$ 线性码 L_1 的最小距离为 3,由前面结果知,L_1 是一个能纠一个差错的纠错码.

L_1 中的码字 $\boldsymbol{a}$ 恰是满足 $H_1\cdot\boldsymbol{a}^T=\mathbf{0}$ 者.由 H_1 的前三列线性相关,故有 $(1,1,1,0,\cdots,0)\in L_1$,由 H_1 的第 2,3,4 列线性无关,故有 $(0,1,1,1,0,\cdots,0)\notin L_1$.

现在用另一顺序来排列 F^4 中这 15 个非零向量.考察有限域 $GF(2^4)$.依本章中命题 3.5,此域 15 个非零元素组成一个乘法循环群.今找出此循环群

的一个生成元及其在 F=GF(2)上的最小多项式 f(x)，由域论知，f(x)的次数是 4.F 上一次多项式只有 x 和 x+1，而不难知道 F 上的二次不可约多项式只有一个，就是 x^2+x+1. 只要一个 F 上 4 次多项式不被这三个多项式整除，它就是 F 上不可约的. 经试算得 x^4+x+1 是 F 上不可约多项式. 这样 $GF(2^4)=F(\alpha)$，α 是 x^4+x+1 的一个根，即

$$\alpha^4+\alpha+1=0,\text{亦即 }\alpha^4=\alpha+1.$$

这个元素 α 是 $(GF(2^4)\setminus 0,\cdot)$这个循环群的一个生成元码？为此要看一下 α 的幂是否穷尽 $GF(2^4)$的所有非零元，今计算如下(把出现的 α^4 都换成 $\alpha+1$)：

$$\alpha^4=1+\alpha,$$
$$\alpha^5=(1+\alpha)\alpha=\alpha+\alpha^2,$$
$$\alpha^6=(\alpha+\alpha^2)\alpha=\alpha^2+\alpha^3,$$
$$\alpha^7=(\alpha^2+\alpha^3)\alpha=\alpha^3+\alpha^4=1+\alpha+\alpha^3.$$

如此计算下去，若令 $\boldsymbol{\alpha}=(1,\alpha,\alpha^2,\alpha^3)$，则得

$$\begin{aligned}
\alpha^{15}=\alpha^0&=\boldsymbol{\alpha}(1000)^T, & \alpha^1&=\boldsymbol{\alpha}(0100)^T, & \alpha^2&=\boldsymbol{\alpha}(0010)^T,\\
\alpha^3&=\boldsymbol{\alpha}(0001)^T, & \alpha^4&=\boldsymbol{\alpha}(1100)^T, & \alpha^5&=\boldsymbol{\alpha}(0110)^T,\\
\alpha^6&=\boldsymbol{\alpha}(0011)^T, & \alpha^7&=\boldsymbol{\alpha}(1101)^T, & \alpha^8&=\boldsymbol{\alpha}(1010)^T,\\
\alpha^9&=\boldsymbol{\alpha}(0101)^T, & \alpha^{10}&=\boldsymbol{\alpha}(1110)^T, & \alpha^{11}&=\boldsymbol{\alpha}(0111)^T,\\
\alpha^{12}&=\boldsymbol{\alpha}(1111)^T, & \alpha^{13}&=\boldsymbol{\alpha}(1011)^T, & \alpha^{14}&=\boldsymbol{\alpha}(1001)^T.
\end{aligned}$$

注意到元素 $1,\alpha,\alpha^2,\alpha^3$ 在 F 上线性无关，上表中，除 $\alpha^{15}=\alpha^0=1$ 外，α 的不同幂彼此也不同，这说明 α 是 15 阶循环群$(GF(2^4)\setminus 0,\cdot)$的一个生成元. 同时也看到 α^i，$0\leqslant i\leqslant 14$，的坐标向量穷尽了 F^4 中所有非零向量.

今把 F^4 的 15 个非零向量按照它所相应的 α 的幂的顺序排列之，便得校验矩阵

$$H_2=\begin{pmatrix}
1&0&0&0&1&0&0&1&1&0&1&0&1&1&1\\
0&1&0&0&1&1&0&1&0&1&1&1&1&0&0\\
0&0&1&0&0&1&1&0&1&0&1&1&1&1&0\\
0&0&0&1&0&0&1&1&0&1&0&1&1&1&1
\end{pmatrix}.$$

如果把 α^i 和它的坐标向量等同起来，也可把 H_2 记作

$$H_2=(1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7,\alpha^8,\alpha^9,\alpha^{10},\alpha^{11},\alpha^{12},\alpha^{13},\alpha^{14}).$$

现在看一下以 H_2 为校验矩阵的(15,11)线性码 L_2 中的码字. 设

$$\boldsymbol{a}=(a_1,a_2,\cdots,a_{14},a_{15})\in L_2,$$

则 $H_2\cdot\boldsymbol{a}^T=\boldsymbol{0}$，这也就是

$$a_1\cdot 1+a_2\cdot\alpha+a_3\cdot\alpha^2+\cdots+a_{14}\cdot\alpha^{13}+a_{15}\cdot\alpha^{14}=0.$$

用 α 乘上等式两侧，并注意到 $\alpha^{15}=1$，便得

$$\alpha_{15}\cdot 1 + a_1\cdot\alpha + a_2\cdot\alpha^2 + a_3\cdot\alpha^3 + \cdots + a_{13}\cdot\alpha^{13} + a_{14}\cdot\alpha^{14} = 0.$$

而这个等式意味着

$$H_2\cdot(a_{15},a_1,a_2,\cdots,a_{13},a_{14})^T = \mathbf{0}.$$

此式说明

$$(a_{15},a_1,a_2,\cdots,a_{13},a_{14})\in L_2.$$

一个线性码 L 中的每一码字,经循环排列后(也就是把每一分量向后错一位,而把最末分量放在第一位置上)得到的字仍是 L 的码字,就称 L 为循环码.这样,我们知道 L_2 是循环码.

循环码是好码,是技术上容易实现的码.

在上面我们已看到$(1,1,1,0,\cdots,0)\in L_1$ 而$(0,1,1,1,0,\cdots,0)\notin L_1$,故 L_1 不是循环码.理论上 L_1 和 L_2 是"同构"的码,实际上它们是由一些不同的材料(向量)组成的,实用中有的好用有的就差一点.这里 L_2 比 L_1 好.称码 L_2 为(15,14)Hamming 码.它是 R.W.Hamming 在 1950 年给出的第一类纠错码.

编码理论是现代通讯理论与基础数学高度结合的一个领域,是基础数学,特别是抽象代数的最直接而又非常深刻的一个应用.上面的简单介绍中,已显示有限域,以及其上的向量空间、矩阵、多项式理论是非常有力的理论和工具。进一步的讨论还将涉及有限域上的代数几何等.应该说,编码理论已成为近年来常提到的"数学技术"的一个组成部分.

对编码理论感兴趣的读者可参看相应的参考书.

练习

1. 给出$(2^3-1,2^3-1-3)=(7,4)$Hamming 码.

2.a) 设$(n,*)$线性码 L 是一个循环码.令

$$I = \{a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1},(a_0,a_1,\cdots,a_{n-1})\in L\}$$

把 I 看作商环 $GF(2)[x]/(x^n-1)$中的子集(即把 $f(x)\in I$ 看成是陪集 $f(x)+(x^n-1)$),则 I 是此商环的一个理想.

b) 设 I 是商环 $GF(2)[x]/(x^n-1)$的一个理想.令

$$L = \{(a_0,a_1,\cdots,a_{n-1}),a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + (x^n-1)\in I\},$$

则 L 是一个$(n,*)$线性码且是一个循环码.

本章习题

1. 设 $[F(\alpha):F]$ 为奇数,则 $F(\alpha)=F(\alpha^2)$.

2. 设 $\mu = i,\nu = \dfrac{2i+1}{i-1}$,求 μ,ν 在 $\mathbb{Q}$ 上的极小多项式.问 $\mathbb{Q}(\mu)$ 与 $\mathbb{Q}(\nu)$ 同构否?

3. 设 K/F 是域扩张,L 是中间域,$\alpha\in K$ 是F 上的代数元,且 α 在F 上有极小多项式

$p(x)$，若 $p(x)$ 是 L 上的不可约多项式，证明 $F(\alpha) \cap L = F$.

4. 设有域扩张链 $F \subseteq L \subseteq E$，$E/L$ 是代数扩域，L/F 是代数扩域，证明：E/F 也是代数扩域.

5. 设 K/F 是扩域，求证下面条件是等价的.

1) K/F 是代数扩域；

2) 满足条件 $F \subseteq A \subseteq K$ 的 K 的任意子环 A 是域.

6. 域 F 的代数扩张 K 的单 F - 自同构必是自同构.

7. 设域 F 的特征不是 2，E/F 是扩域，并且 $[E:F]=4$. 证明：存在一个满足条件 $F \subseteq I \subseteq E$ 的 F 的二次扩域 I 的充分与必要条件是：$E=F(\alpha)$，而 α 在 F 上有极小多项式 x^4+ax^2+b.

8. 设 K/F 为有限次扩域，且 L,H 为中间域，使得 $L(H)=K$，证明：$[K:L] \leqslant [H:F]$.

9. 设 $f(x)=x^4+x^3+x^2+x+1 \in \mathbf{Z}_2[x]$. 求证：

1) $f(x)$ 在 $\mathbf{Z}_2[x]$ 内是不可约的；

2) 设 α 是 $f(x)$ 在 $\mathbf{Z}_2$ 的某个扩域内的一个根，则 $\mathbf{Z}_2(\alpha)=GF(2^4)$ 且 α 不是 15 阶乘法群 $(\mathbf{Z}_2(\alpha)\setminus\{0\},\cdot)$ 的生成元.

10. 构造一个有 9 个元素的域，并且给出它的加法及乘法.

11. p 为素数，$n \geqslant 1$ 且 $n \nmid p^n$. 设 $a \in GF(p)$. 证明：$x^{p^n}-x-a$ 在 $GF(p)$ 上可约.

12. 令 $x^3-a \in \mathbf{Q}[x]$ 是不可约多项式，而 α 是 x^3-a 的一个根，证明：$F(\alpha)$ 不是 x^3-a 在 $\mathbf{Q}$ 上的分裂域中.

13. 设 $p_1,p_2,\cdots,p_r$ 是 r 个不同的素数，且 $E=\mathbf{Q}(\sqrt{p_1},\cdots,\sqrt{p_r})$，求 $\mathrm{Gal}(E/\mathbf{Q})$.

14. 设域 F 的特征不为 3，K 是域 F 上一个三次不可约多项式的一个分裂域，证明：$\mathrm{Gal}(K/F)$ 同构于对称群 S_3 或交代群 A_3.

附录　多元多项式环(代数几何初步)

§1　代数簇

在本章中我们讨论一个代数对象:复数域 $\mathbb{C}$ 上 n 元多项式环 $\mathbb{A}=\mathbb{C}[x_1,\cdots,x_n]$, 它是一个有 1 的交换整环,是唯一分解环;以及一个几何对象:

$$\mathbb{C}^n=\{(c_1,\cdots,c_n)\mid \forall\ c_i\in\mathbb{C}\},$$

称之为 n 维仿射空间,其元素 $(c_1,\cdots,c_n)$ 称之为点;和这两者之间的联系.为简单计,令 $x=(x_1,\cdots,x_n)$ 而把 $\mathbb{A}=\mathbb{C}[x_1,\cdots,x_n]$ 中的多项式 $f(x_1,\cdots,x_n)$ 记作 $f(x)$. 令 $c=(c_1,\cdots,c_n)\in\mathbb{C}^n$, 而把 $f(c_1,\cdots,c_n)$ 记作 $f(c)$. 当 $f(c)=0$ 时称点 c 为多项式 f 的一个零点.任取有限个多项式 $f_i(x_1,\cdots,x_n)\in\mathbb{A}, i=1,\cdots,m$, 而考察联立方程组

$$\begin{cases}f_1(x_1,\cdots,x_n)=0,\\ \cdots\cdots\cdots\cdots\cdots\cdots\\ f_m(x_1,\cdots,x_n)=0\end{cases}\qquad (*)$$

的解的全体,也就是 $f_1,\cdots,f_m$ 的所有共同零点的全体 $\mathbb{V}(f_1,\cdots,f_m)\subseteq\mathbb{C}^n$. 这是一个非常重要的问题.这个问题也把环 $\mathbb{A}$ 的有限子集 $\{f_1,\cdots,f_m\}$ 和仿射空间 $\mathbb{C}^n$ 的子集 $\mathbb{V}(f_1,\cdots,f_m)$ 紧密地联系起来.

如果所有 f_i 是 $x_1,\cdots,x_n$ 的一次多项式,则由线性方程组理论我们知道 $\mathbb{V}(f_1,\cdots,f_m)$ (当它不空时)是 $\mathbb{C}$ 上 n 维向量空间 $\mathbb{C}^n$ 的一个子空间 V 的陪集 $(a_1,\cdots,a_n)+V$. 当 $m=1, n=2$ 或 3 时,即只讨论一个方程 $f(x_1,x_2)=0$ 或 $f(x_1,x_2,x_3)=0$, 且当多项式 f 的次数是 2 时,这 $\mathbb{V}(f)$ 就是我们在解析几何中研究的二次曲线和二次曲面.对于一般情况可以想象 $\mathbb{V}(f_1,\cdots,f_m)$ 是一个很复杂的数学研究对象.由于 f_i 的非线性性,虽然 $\mathbb{V}(f_1,\cdots,f_m)$ 是 $\mathbb{C}^n$ 的子集,但 $\mathbb{C}$ - 向量空间 $\mathbb{C}^n$ 中的算法(加法和数乘)对它没有什么意义了. $\mathbb{V}(f_1,\cdots,f_m)$ 是内容丰富,深刻的代数几何的主要研究对象.本书中只能作极初步的介绍.

定义 1.1　设 J 是 $\mathbb{A}$ 中的一个任意(不一定是有限的)子集,称 J 中多项式的共同零点集 $\mathbb{V}(J)$, 亦即

$$\mathbb{V}(J)=\{c\in\mathbb{C}^n \mid \forall\ f\in J, f(c)=0\},$$

为一个代数簇(或简称簇).就是说 $\mathbb{C}^n$ 的一个子集 $\mathbb{V}$ 被称为代数簇,如果存在 $J\subseteq\mathbb{A}$ 使得 $\mathbb{V}=\mathbb{V}(J)$. $\mathbb{V}(J)$ 常说成是 J 的零点集.

命题 1.2　1)设 $J_1\subseteq J_2\subseteq\mathbb{A}$, 则 $\mathbb{V}(J_1)\supseteq\mathbb{V}(J_2)$.

2) 设 J 是 $\mathbb{A}$ 的子集, $I=(J)$, 则有 $\mathbb{V}(J)=\mathbb{V}(I)$.

证明　1) 是显然的.今证 2).任取 $g\in I=(J)$, 则由理想 I 的定义,有

$$g=g_1f_1+\cdots+g_if_i,\forall\ f_j\in J, g_j\in\mathbb{A},$$

因而 $\mathbb{V}(J)$ 中的点(即 J 中多项式的共同零点)也必是 g 的零点,随之 $\mathbb{V}(J)\subseteq\mathbb{V}(I)$. 另一方面, $J\subseteq I$, 根据 1)有 $\mathbb{V}(J)\supseteq\mathbb{V}(I)$, 故得 $\mathbb{V}(J)=\mathbb{V}(I)$. □

上命题是说,在讨论代数簇时,用理想 I 去代替子集 J, 我们没有任何损失.

下面将把代数簇这个几何对象与一个代数对象——理想对应起来,可把它看作是圆、椭圆、抛物线、双曲线与二元二次多项式间相互对应的深化,也可看作是另一类 Galois 对应:在不同类型的对象之间建立漂亮的对应关系.

定义 1.3　设 U 是仿射空间 $\mathbb{C}^n$ 的一个子集,规定

$$\mathbb{I}(U)=\{f\in\mathbb{A}\mid\forall\ c\in U, f(c)=0\},$$

即 $\mathbb{I}(U)$ 是以 U 中所有点为零点的一切多项式的集合.

容易证明: $\mathbb{I}(U)$ 是环 $\mathbb{A}$ 的一个理想,以及当 $U_1\subseteq U_2$ 时,有 $\mathbb{I}(U_1)\supseteq\mathbb{I}(U_2)$. 由上面这两个定义,我们得到下面的两个对应:

$$\begin{aligned}\mathbb{I}:\{\mathbb{C}^n\text{ 中的所有簇}\} &\longrightarrow \{\mathbb{A}\text{ 的所有理想}\} \\ V &\longmapsto \mathbb{I}(V);\end{aligned}\qquad(1)$$

$$\begin{aligned}\mathbb{V}:\{\mathbb{A}\text{ 的所有理想}\} &\longrightarrow \{\mathbb{C}^n\text{ 中的所有簇}\} \\ I &\longmapsto \mathbb{V}(I).\end{aligned}\qquad(2)$$

$\mathbb{I}$ 和 $\mathbb{V}$ 是一一对应吗? $\mathbb{I}$ 和 $\mathbb{V}$ 是互逆对应吗?为此先看

命题 1.4

1) 对任意簇 $V=\mathbb{V}(I)$ 有 $\mathbb{V}(\mathbb{I}(V))=V$;

2) 对任意理想 I, 有 $\mathbb{I}(\mathbb{V}(I))\supseteq I$;

3) 对任意理想 $I=\mathbb{I}(V)$, 其中 V 是簇,有 $\mathbb{I}(\mathbb{V}(I))=I$.

证明　1) 依 $\mathbb{V}$ 的定义,显然有 $\mathbb{V}(\mathbb{I}(V))\supseteq V$. 另一方面,设 $V=\mathbb{V}(I)$, 则易见 $\mathbb{I}(V)\supseteq I$. 于是 $\mathbb{V}(\mathbb{I}(V))\subseteq\mathbb{V}(I)=V$, 故 $\mathbb{V}(\mathbb{I}(V))=V$.

2) 是显然的.

3) 已知 $I=\mathbb{I}(V)$, 由 1)知 $\mathbb{V}(I)=\mathbb{V}(\mathbb{I}(V))=V$, 随之 $\mathbb{I}(\mathbb{V}(I))=\mathbb{I}(V)=I$. □

$I=\mathbb{I}(V)$ 的意义是: I 是以簇 V 中点为零点的所有多项式的全体,尽管

以簇 V 中点为零点的理想不是唯一的，然而 I 是包含所有这些理想的那个理想，即是有此性质的最大的那个理想. 为引用方便，我们引入

定义 1.5 称 $\mathbb{A}$ 的理想 I 为 V －理想，如果 $I = \mathbb{I}(V)$，V 是簇.

下面我们将看到，并不是 $\mathbb{A}$ 的所有理想都是 V －理想. 这样欲使 $\mathbb{I}$，$\mathbb{V}$ 是一一对应，互逆对应，需对其定义域或值域进行修正如下：

$$\begin{aligned} \mathbb{I}: \{V\} = \{\mathbb{C}^n \text{ 中所有簇}\} &\longrightarrow \{\mathbb{A} \text{ 的所有 } V-\text{理想}\} = \{I\} \\ V &\longmapsto \mathbb{I}(V); \end{aligned} \tag{3}$$

$$\begin{aligned} \mathbb{V}: \{I\} = \{\mathbb{A} \text{ 的所有 } V-\text{理想}\} &\longrightarrow \{\mathbb{C}^n \text{ 中的所有簇}\} = \{V\} \\ I &\longmapsto \mathbb{V}(I). \end{aligned} \tag{4}$$

综合上面的讨论便得

定理 1.6 $\mathbb{A} = \mathbb{C}[x_1, \cdots, x_n]$. 令

$$\{I\} = \{\mathbb{A} \text{ 的所有 } V-\text{理想}\} \underset{\mathbb{I}}{\overset{\mathbb{V}}{\rightleftarrows}} \{\mathbb{C}^n \text{ 中的所有簇}\} = \{V\}$$

如(3)(4). 则有

1) $\mathbb{V}(\mathbb{I}(V)) = V$，其中 V 是 $\mathbb{C}^n$ 中的簇；

2) $\mathbb{I}(\mathbb{V}(I)) = I$，其中 I 是 $\mathbb{A}$ 的 V －理想；

3) $\mathbb{V}$，$\mathbb{I}$ 是一一对应且是互逆对应；

4) 若 $V_1, V_2 \in \{V\}$ 且 $V_1 \subseteq V_2$，则 $\mathbb{I}(V_1) \supseteq \mathbb{I}(V_2)$；

5) 若 $I_1, I_2 \in \{I\}$ 且 $I_1 \subseteq I_2$，则 $\mathbb{V}(I_1) \supseteq \mathbb{V}(I_2)$. □

如果说人们利用 Galois 基本定理中的 Galois 对应(扩域 K/F 的中间域集与其 Galois 群的子群集之间的一一对应)，用较容易控制的有限群去研究扩域 K/F 的性质，则现在上面定理中所提供的对应 $\mathbb{V}$，$\mathbb{I}$，将帮助我们用较容易控制的理想论(代数理论)去研究簇(几何对象)的性质. 在下面两节中将对此作极初步的讨论.

下面是一些简单的例子.

容易证明理想 (0)，$(x_1 - c_1, \cdots, x_n - c_n)$(注意到它是 $\mathbb{A}$ 的极大理想)，$\mathbb{A}$ 是 V －理想. 我们有

$$\begin{aligned} \{I\} &\underset{\mathbb{I}}{\overset{\mathbb{V}}{\longleftrightarrow}} \{V\} \\ (0) &\longleftrightarrow \mathbb{C}^n \\ (x_1 - c_1, \cdots, x_n - c_n) &\longleftrightarrow \{(c_1, \cdots, c_n)\} \\ \mathbb{A} &\longleftrightarrow \varnothing(\text{空集}). \end{aligned}$$

在本节末我们想介绍一下关于 $\mathbb{C}$ 上多元多项式组成的联立方程组的“代数基本定理”——Hilbert 零点定理. 为此我们从 V －理想入手.

命题 1.7 V - 理想 $I=\mathbb{I}(V)$，V 是簇，满足性质：对任意 $f\in\mathbb{A}$，若 f 的一个幂 $f^m\in I$，则 $f\in I$.

证明 若 $f^m\in I=\mathbb{I}(V)$，则对任意 $c\in V$，有 $(f(c))^m=0$，随之 $\forall\ c\in V, f(c)=0$，依 $\mathbb{I}(V)$ 的定义知 $f\in\mathbb{I}(V)=I$. □

定义 1.8 设 I 是环 $\mathbb{A}$ 的理想，规定

$$\sqrt{I}=\{f\in\mathbb{A}\mid f\text{ 的一个幂 }f^m\in I\},$$

易见 $I\subseteq\sqrt{I}$ 且 $\sqrt{I}$ 也是一个理想. 称 $\sqrt{I}$ 为理想 I 的根理想. 称 $I=\sqrt{I}$ 的理想 I 为根闭理想.

这样 V - 理想是根闭理想. 显然不是所有理想都是根闭理想，例如 $((x_1+1)^8)$ 就不是根闭理想，随之，也不是 V - 理想.

下面我们给出

Hilbert **零点定理** 设 I 是 $\mathbb{A}=\mathbb{C}[x_1,\cdots,x_n]$ 的一个理想，则 $\mathbb{I}(\mathbb{V}(I))=\sqrt{I}$.

Hilbert **零点定理(弱形式)** 设 I 是 $\mathbb{A}=\mathbb{C}[x_1,\cdots,x_n]$ 的一个不等于 $\mathbb{A}$ 的理想，则 $\mathbb{V}(I)$ 不空.

上面这两定理的证明以及它们互相等价的证明，都略去. 有兴趣的读者请看相应的书.

Hilbert 零点定理对于代数几何的重要性和基础性相当于代数基本定理之于一元代数方程式论. 后者是说，一个复系数正次数一元多项式(即可能有根的多项式)必在复数域 $\mathbb{C}$ 中有根. 现在让我们回到本节初的联立方程组 $(*)$，它的解集就是 $\mathbb{V}(f_1,\cdots,f_m)$. 我们已经知道

$$\mathbb{V}(f_1,\cdots,f_m)=\mathbb{V}((f_1,\cdots,f_m)),$$

如果理想 $(f_1,\cdots,f_m)=\mathbb{A}$，即有 $g_i\in\mathbb{A}$ 使

$$g_1f_1+\cdots+g_mf_m=1,$$

此时当然 $(*)$ 根本不可能有解. Hilbert 零点定理(弱形式)是说，只要 $I=(f_1,\cdots,f_m)\neq\mathbb{A}$，即是联立方程组 $(*)$ 可能有解时，则 $\mathbb{V}(I)$ 不空，即方程组 $(*)$ 在 $\mathbb{C}^n$ 中有解. 在可能有解时，肯定必在 $\mathbb{C}$ (或 $\mathbb{C}^n$)中有解，这就是代数基本定理和 Hilbert 零点定理所作的重要结论.

作为 Hilbert 零点定理的一个直接推论，我们还有：根闭理想是 V - 理想. 这样，有了 Hilbert 零点定理之后，根闭理想和 V - 理想就是相同的概念了.

§2 Hilbert 基定理

在上一节中我们再一次地看到环的理想这一概念的重要性. 这一次是和

重要几何对象——簇相联系而出现的. 以前,它曾和环的同态相联系,以及和代数整数分解相联系而出现过两次. 同一概念在不同的场合中都出现,这说明理想这一概念的内涵丰富多采.

本节我们给出环 $\mathbb{A} = \mathbb{C}[x_1, \cdots, x_n]$ 的理想的一个重要性质: $\mathbb{A}$ 的每一理想都是有限生成的. 这个有广泛影响的 Hilbert 基定理是代数几何的另一基石. 首先讨论此性质的一个等价形式. 为此引入

定义 2.1 R 是有 1 的交换环,称 R 为 Noether 环,如果对 R 中任意递增理想链: I_i 是 R 的理想

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots \tag{5}$$

必存在正整数 N 使得

$$I_N = I_{N+1} = \cdots$$

常把此性质说成理想链(5)在有限步上停下来.

例 域 F 上一元多项式环 $F[x]$ 是 Noether 环.

设 I_i 是 $F[x]$ 的理想且

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$$

设 $I = \bigcup_{n=1}^{\infty} I_n$, 则易知(证明!) I 是 $F[x]$ 的理想. 但 $F[x]$ 是主理想整环,故 $I = (f(x))$. 注意到 I 是诸 I_n 之并集,故 $f(x)$ 必属于某一 I_N. 随之便有

$$((f(x)) \subseteq I_N \subseteq I_{N+1} \subseteq \cdots \subseteq I = (f(x)),$$

即证得 $(f(x)) = I_N = I_{N+1} = \cdots$ □

命题 2.2 设 R 是有 1 的交换环. R 是 Noether 环当且仅当 R 的每一理想都是有限生成的(有限生成的理想也常说成是有有限基的理想).

证明 1) 设 R 是 Noether 环. 若 R 有理想 I 不是有限生成的,则在 I 中必有无限多个元素: $a_1, a_2, \cdots, a_n, \cdots$, 使得

$$(a_1) \subsetneq (a_1, a_2) \subsetneq (a_1, a_2, a_3) \subsetneq \cdots \subsetneq (a_1, \cdots, a_n) \subsetneq \cdots$$

这与 R 是 Noether 环是矛盾的,故 R 的每一理想有有限基.

2) 读者仿照上例的证明思路去证明另一方面. □

Hilbert **基定理** 域 F 上 n 元多项式环 $F[x_1, \cdots, x_n]$ 是 Noether 环.

它是下面命题的简单推论.

命题 2.3 设 R 是有 1 的交换环,且是 Noether 环,则 $R[x]$ 也是 Noether 环.

证明 依上命题,为此只需证明,环 $R[x]$ 的任意理想 I 必有有限基,即有 I 中的一个有限子集 $\{a_1, a_2, \cdots, a_n\}$ 使任一 $a \in I$ 有

$$a = g_1 a_1 + \cdots + g_n a_n,$$

其中 $g_i \in R[x]$. $R[x]$ 中任一非零元素 a 都可唯一地表成

$$a = r_t x^t + \cdots + r_1 x + r_0,$$

其中 $r_i \in R, r_t \neq 0$. 把 a 的次数 t 记作 $\deg a$, a 的首项 $r_t x^t$ 记作 $LT(a)$, 而首项系数 r_t 记作 $CLT(a)$.

今考察下列 R 中集合

$$I_k = \{CLT(a) \mid \deg a = k, a \in I\} \cup \{0\},$$

即 I_k 是 I 中所有 k 次多项式的首项系数以及 0 组成的集合. 注意 I 是 $R[x]$ 的理想, 从而易知 I_k 是环 R 的理想. 依 R 是 Noether 环, 每一理想 I_k, k 是任意非负整数, 都有一个有限基: $r_{k,1}, \cdots, r_{k,m_k}$. 注意到 I_k 的定义, 知必有 I 的 k 次多项式 $a_{k,i}$ 使得对任意 i, 有 $CLT(a_{k,i}) = r_{k,i}$. 并且对 I 中任一 k 次多项式 a_k, 由于 $CLT(a_k) \in I_k$, 故 $CLT(a_k)$ 必可表成理想 I_k 的有限基的线性和, 即

$$CLT(a_k) = r_1 \cdot r_{k,1} + \cdots + r_{m_k} \cdot r_{k,m_k}, \ r_i \in R,$$

随之

$$b = a_k - (r_1 \cdot a_{k,1} + \cdots + r_{m_k} \cdot a_{k,m_k}) \in I$$

是 I 中一个次数为 $s \leqslant k-1$ 的多项式. 如果对 b 代替 a_k, 重复上面步骤(即用诸 $a_{s,i}$ 的首项系数去"消去"给定多项式的首项系数), 最多有限次后, 必得

$$a_k = r_{k,1} \cdot a_{k,1} + \cdots + r_{k,m_k} \cdot a_{k,m_k} + \cdots$$
$$+ r_{0,1} \cdot a_{0,1} + \cdots + r_{0,m_0} \cdot a_{0,m_0}.$$

上面讨论说明 I 中所有次数小于等于某固定 k 的多项式, 都可通过 I 中有限集 $G_k = \{a_{s,i_s} \mid 1 \leqslant s \leqslant k, 1 \leqslant i_s \leqslant m_s\}$ 线性表示. 但 I 中元素的次数是可以任意的. 下面我们想办法处理这种情况. 考虑 R 中子集

$$J = \{CLT(a) \mid a \in I\} \cup \{0\},$$

即 J 是 I 中所有多项式的首项系数的集合(含 0). 今证 J 也是 R 的理想.

设 $u, v \in J$. 依 J 的定义有

$$u = CLT(a), v = CLT(b), a, b \in I.$$

令 $\deg a = s, \deg b = t$, 则 ax^t, bx^s 仍在 I 中, 且它们有相同的次数 $s+t$, 这样 $ax^t + bx^s \in I$. 故

$$u \pm v = CLT(ax^t \pm bx^s), \text{或 } 0,$$

随之 $u \pm v \in J$. 又若 $r \in R, u \in J$, 则显然有 $ru \in J$. 总起来, 就知 J 是 R 的理想.

由于 R 是 Noether 环, 其理想 J 必有有限基: $u_1, u_2, \cdots, u_m$. 依 J 的定义, I 中必有元素 $a_1, \cdots, a_m$ 使得 $CLT(a_i) = u_i, 1 \leqslant i \leqslant m$. 为醒目计, 不妨认定诸 $\deg a_i$ 相同, 都是 t (不然的话, 可对一些 a_i 适当乘以 x 的幂).

任取 I 中元素 a，其 $\deg a = t+s \geqslant t$，$CLT(a) \in J$，故它必可表成 J 的有限基的线性和，即有

$$CLT(a) = h_1u_1 + \cdots + h_mu_m,\ h_i \in R.$$

这样 $a' = a - (h_1x^s \cdot a_1 + \cdots + h_mx^s \cdot a_m) \in I$ 且 $\deg a' \leqslant \deg a - 1$. 如果仍有 $\deg a' \geqslant t$，则对 a' 重复上面步骤(即用诸 a_i 的首项系数去“消去” a' 的首项系数)，最多这样重复 s 次，必达到

$$b = a - (g_1 \cdot a_1 + \cdots + g_m \cdot a_m) \in I,$$

其中所有的 $g_i \in R[x]$ 且 $\deg b < t$. 这就是说，对 I 中任意次数多项式 a，可利用 I 中有限个元素 $a_1,\cdots,a_m$ 的线性和把多项式 a 的次数降到小于 t. 而 I 中次数 $\leqslant t-1$ 多项式又可如上面通过 I 中有限集 G_{t-1} 的线性和表示出来. 这样理想 I 有有限基 $\{a_1,\cdots,a_n\} \cup G_{t-1}$. □

Hilbert **基定理的证明**　显然域 F 是 Noether 环，依上命题得 $F[x]$ 是 Noether 环，随之 $F[x_1][x_2] = F[x_1,x_2]$ 也是. 再用一下归纳法就得定理的证明. □

如果比较一下我们过去对 $F[x]$ 是主理想环的证明和上面命题的证明，或可使我们对后者有“似曾相识”之感，即 Hilbert 基定理的美妙证明思路(用一些多项式的首项去消另一多项式的首项)已在 $F[x]$ 是主理想环的证明中可以察觉到.

Hilbert 基定理是说 $F[x_1,\cdots,x_n]$ 的理想有有限基，但并没有把它们找出来，它是一个“理论上”的存在定理. 关于它有一段史话. P. A. Gordan (1837—1912)在研究不变量理论时需要对多元多项式环的理想证明它有有限基，在 1868 年他用一个既长又复杂而极富技巧的计算方法对二元多项式环的一个给定理想，找出它的一个特定有限基，之后，很多数学家按 Gordan 的计算路子去考察一般 n 元情况，由于太复杂而未获成功. 忽然 Hilbert 在 1888 年发表的一短文，证明任意 n 元多项式环的任意理想都有有限基. 这件事很难被接受，特别当时数学界对存在定理的理解只是：只有当你找到它，它才是存在的. 有人怀疑 Hilbert 基定理是否是数学. 反应最强烈的当然是 Gordan，他说这个定理证明似乎和神学中证明上帝的存在很相似，“Das ist nicht Mathematik. Das ist Theologie”(这不是数学，这是神学). 当然，今天数学界对纯粹的存在定理和构造性存在定理都早已接受并都已习惯了.

§3　代数簇的分解

在 §1 中我们建立了下面的一一对应：

$$\{I\} = \{\mathbb{A}\text{ 的所有 }V-\text{理想}\} \underset{\mathbb{I}}{\overset{\mathbb{V}}{\rightleftarrows}} \{\mathbb{C}^n\text{ 中的所有簇}\} = \{V\},$$

显然$\{\{I\},\subseteq\}$(其中$\subseteq$是指 V - 理想之间的包含关系)和$\{\{V\},\subseteq\}$(其中$\subseteq$是指簇之间的包含关系)都是偏序集,而对应 $\mathbb{V},\mathbb{I}$ 是这两个偏序集之间的反同构对应.这两个偏序集还是格.我们只给出关于$\{\{V\},\subseteq\}$是格的证明,而把利用 $\mathbb{V},\mathbb{I}$ 是反同构对应来证明$\{\{I\},\subseteq\}$是格的工作留给读者.为此只需证明 $V_1\cup V_2$ 是簇,即两的簇并集是簇,以及 $V_1\cap V_2$ 是簇,即两个簇的交集也是簇.证明 $\mathbb{C}^n$ 的一个子集 V 是簇,依定义,需证有 $S\subseteq\mathbb{A}$ 使得 $V=\mathbb{V}(S)$.今证

命题 3.1　设 $V_1=\mathbb{V}(I_1), V_2=\mathbb{V}(I_2)$,其中 I_1,I_2 是 $\mathbb{A}$ 的理想.则有

1) $V_1\cap V_2=\mathbb{V}(I_1+I_2)=\mathbb{V}(I_1)\cap\mathbb{V}(I_2)$;

2) $V_1\cup V_2=\mathbb{V}(I_1I_2)=\mathbb{V}(I_1\cap I_2)=\mathbb{V}(I_1)\cup\mathbb{V}(I_2)$;

3) 两簇之并集或交集都是簇.

证明　1) 若 $c=(c_1,\cdots,c_n)\in V_1\cap V_2$,则 $c\in V_1$ 且 $c\in V_2$,随之对任意 $f_1\in I_1, f_2\in I_2$,有 $f_1(c)=0, f_2(c)=0$,因而 $(f_1+f_2)(c)=f_1(c)+f_2(c)=0+0=0$,即 $c\in\mathbb{V}(I_1+I_2)$.反过来,若 $c\in\mathbb{V}(I_1+I_2)$,则对任意 $f_1\in I_1\subseteq I_1+I_2, f_2\in I_2\subseteq I_1+I_2$,有 $f_1(c)=0, f_2(c)=0$,即 $c\in\mathbb{V}(I_1)$ 且 $c\in\mathbb{V}(I_2)$,随之 $c\in\mathbb{V}(I_1)\cap\mathbb{V}(I_2)=V_1\cap V_2$;

2) 先证 $V_1\cup V_2=\mathbb{V}(I_1I_2)$.由于 $I_1\supseteq I_1I_2, I_2\supseteq I_1I_2$,故由定理 1.6 有

$$V_1=\mathbb{V}(I_1)\subseteq\mathbb{V}(I_1I_2), V_2=\mathbb{V}(I_2)\subseteq\mathbb{V}(I_1I_2),$$

随之有 $V_1\cup V_2\subseteq\mathbb{V}(I_1I_2)$.另一方面,设 $c=(c_1,\cdots,c_n)\in\mathbb{V}(I_1I_2)$ 而 $c\notin V_1$,则必有 $c\in V_2$.这是因为,此时必有 $f\in I_1, 0\neq f(c)\in\mathbb{C}$.任取 $g\in I_2$,则由关于 c 的假设知 $f(c)g(c)=0$,随之 $g(c)=0$,这说明 $c\in\mathbb{V}(I_2)=V_2$.总起来就得:$V_1\cup V_2=\mathbb{V}(I_1I_2)$.

注意到 $I_1I_2\subseteq I_1\cap I_2\subseteq I_i, i=1,2$,再依定理 1.6,得 $V_1\cup V_2=\mathbb{V}(I_1I_2)\supseteq\mathbb{V}(I_1\cap I_2)\supseteq V_1\cup V_2$,即 $\mathbb{V}(I_1I_2)=\mathbb{V}(I_1\cap I_2)$.

3)是 1),2)的直接推论.□

这样,我们知对应 $\mathbb{V},\mathbb{I}$ 是格$\{\{I\},\subseteq\}$与格$\{\{V\},\subseteq\}$之间的反同构.因而可自然地把它看成另一个 Galois 对应.

现在来讨论簇的分解.先引入

定义 3.2　1) 称非空簇 V 为不可约的,如果 V 不能表成两个非空簇 $V_1\neq V, V_2\neq V$ 之并 $V_1\cup V_2$,即是说,若 $V=V_1\cup V_2$,则 $V=V_1$ 或 $V=V_2$.否则,则称 V 是可约簇.

2) 称 V - 理想 I 为不可约的,如果 I 不能表成两个(根闭)理想 I_1,I_2 之

交，其中 $I_i \neq \mathbb{A}, I_i \neq I, i = 1,2$，即是说，若 $I = I_1 \cap I_2$，则 $I = I_1$ 或 $I = I_2$. 否则就称 I 为可约理想.

如果把簇(理想)比作整数，把"并"("交")比作数的乘法，则不可约簇(不可约理想)相当于素数，空簇($\mathbb{A}$)相当于单位 ± 1，算术基本定理的对应物将是把一个簇分解成一些不可约簇的并，或是把一个理想分解成一些不可约理想的交，而本节开始时的讨论说明后两者是关系密切的.

下面我们用 Hilbert 基定理来证明簇分解的存在性.

Hilbert 基本定理是说：理想升链在有限处停止. 把它翻译到偏序集 $\{\{V\}, \subseteq\}$ 上去，这就是下面

命题 3.3 簇降链

$$V_1 \supseteq V_2 \supseteq V_2 \supseteq \cdots \supseteq V_n \supseteq \cdots \tag{1}$$

必在有限处停止，亦即存在 N，使得

$$V_N = V_{N+1} = \cdots$$

证明 由簇降链(1)，得理想升链

$$\mathbb{I}(V_1) \subseteq \mathbb{I}(V_2) \subseteq \cdots \subseteq \mathbb{I}(V_n) \subseteq \cdots$$

依 Hilbert 基定理，存在 N 使

$$\mathbb{I}(V_N) = \mathbb{I}(V_{N+1}) = \cdots$$

再用 $\mathbb{V}$ 把它对应回去，便是

$$V_N = V_{N+1} = \cdots \quad \square$$

设有 V，它是一个非空簇，且 V 不能表成有限个不可约簇的并，我们希望由此得到矛盾. 显然 V 本身不是不可约的，这样 $V = W_1 \cup W_2$，非空簇 $W_i \subsetneq V, i = 1,2$，$W_i$ 中必有一，比如说是 W_1，不能表成有限个不可约簇的并，否则将与对 V 的假设矛盾. 设 $V_1 = W_1 \subsetneq V$，而对 V_1 重复对 V 的讨论，这样将得非空簇 $V_2 \subsetneq V_1$，且 V_2 和 V_1 (以及 V)有同样的性质. 这样继续讨论下去，便得无限降链

$$V \supsetneq V_1 \supsetneq V_2 \supsetneq \cdots \supsetneq V_n \supsetneq \cdots$$

这和刚证的命题是矛盾的. 这就证明了下面

定理 3.4 (簇分解的存在性定理) 任一非空簇 V 都可表成有限个不可约簇的并：

$$V = V_1 \cup V_2 \cup \cdots \cup V_n, \tag{2}$$

其中每个 V_i 是不可约簇. V 的表示(2)当然不是唯一的，例如可让 V_1 重复出现多次而得 V 的另外一些表示. 称 V 的分解(2)为最简分解，如果(2)中任意 V_i 都是不能去掉的.

定理 3.5(簇分解的唯一性) 设非空簇 V 有两个最简分解

$$V = V_1 \cup V_2 \cup \cdots \cup V_n = W_1 \cup W_2 \cup \cdots \cup W_m,$$

其中 V_i, W_j 都是不可约簇,则 $n = m$ 且对 W_i 适当重编号后有 $V_i = W_i, i = 1,2,\cdots,n$.

证明 任取某一 W_i,比如说是 W_1. 由 $W_1 \subseteq V$ 得

$$W_1 = W_1 \cap V = (W_1 \cap V_1) \cup (W_1 \cap V_2) \cup \cdots \cup (W_1 \cap V_n),$$

由于 W_1 是不可约的,故必有 i. 使

$$W_1 = W_1 \cap V_i \subseteq V_i.$$

对 V_i 进行同样讨论,则必有 j, 使

$$V_i = V_i \cap W_j \subseteq W_j,$$

这样 $W_1 \subseteq V_i \subseteq W_j$. 但 V 的两个分解都是最简分解,不同的 W_i 是不能有包含关系的,故 $j = 1$, 而 $W_1 = V_i$. 对 W_2 进行上述讨论,便有 $W_2 = V_j$,且易见 $i \neq j$. 如此继续下去便得定理的结论.□

可以说,有限交换群的唯一分解定理完全地刻画了有限交换群的结构,因为那里的"基本构件"是 p^n 阶循环群,而它的结构是清楚的.但这里,簇的唯一分解定理只是把对簇的研究归结为对不可约簇的研究,虽然这是重大的步骤,但对簇的研究却远没有完成.因为不可约簇仍是一个很复杂的对象.下面我们只限于看一下,不可约簇 V 对应的理想 $\mathbb{I}(V)$ 是个什么样子.

引理 3.6 若 I,J 是 $\mathbb{A}$ 的理想, I 是 V - 理想且 $\mathbb{V}(I) = \mathbb{V}(J)$, 则 $I \supseteq J$.

证明 由 $\mathbb{V}(I) = \mathbb{V}(J)$, 得 $\mathbb{IV}(I) = \mathbb{IV}(J)$. 由于 I 是 V - 理想,故有 $\mathbb{IV}(I) = I$. 另一方面 $\mathbb{I}(\mathbb{V}(J)) \supseteq J$, 这是因为 $\mathbb{I}(\mathbb{V}(J))$ 是在 $\mathbb{V}(J)$ 上取零值的最大的那个理想,而 J 只是在 $\mathbb{V}(J)$ 上取零值的一个理想.总起来便是 $I = \mathbb{IV}(I) = \mathbb{IV}(J) \supseteq J$. □

命题 3.7 $I = \mathbb{I}(V)$, V 是不可约簇,是素理想.

证明 今用反证法,而设 I 不是素理想.这样必有元素 $a \in \mathbb{A} \setminus I, b \in \mathbb{A} \setminus I$ 而 $ab \in I$. 此时 $I \subsetneq I_1 = I + (a), I \subsetneq I_2 = I + (b)$. 注意到 I 是 V - 理想, 依引理,有

$$V_i = \mathbb{V}(I_i) \subsetneq \mathbb{V}(I) = V, i = 1,2.$$

随之 $V_1 \cup V_2 \subseteq V$. 另一方面,由于 $ab \in I$, 易得 $I_1 I_2 \subseteq I$. 再依命题 1.4, 得

$$V = \mathbb{V}(I) \subseteq \mathbb{V}(I_1 I_2) = \mathbb{V}(I_1) \cup \mathbb{V}(I_2) = V_1 \cup V_2.$$

总起来,得

$$V = V_1 \cup V_2, V_1 \neq V, V_2 \neq V.$$

这和 V 是不可约簇相矛盾,故 I 是素理想.□

一个自然的问题是,上命题之逆是否成立,即是否 $\mathbb{A}$ 的任一素理想 I 都可表为 $I = \mathbb{I}(V)$, V 是不可约簇. 回答是肯定的,但其证明要用到 Hilbert 零点定理. 利用 Hilbert 零点定理的结论: $\mathbb{IV}(I) = \sqrt{I}$, 我们很容易证明:在 $\mathbb{C}[x_1,\cdots,x_n]$ 中 V - 理想和根闭理想是等价的概念(这一点前面我们已经提到过). V - 理想是借助于簇而定义的概念,不太好掌握,而根闭理想则完全是一个纯代数(即只用环的语言)的概念,是易验证的. 作为习题,读者不难证明下面两个命题.

命题 3.8　$\mathbb{A}$ 的素理想必是根闭理想(再依 Hilbert 零点定理,也是 V - 理想).

命题 3.9　$\mathbb{A}$ 的素理想必是不可约理想.

由上命题便得命题 3.7 之逆是成立的.

这里顺便指出,利用 Hilbert 零点定理不难证明: $\mathbb{A}$ 中的极大理想是且仅是形如 $(x_1 - c_1, x_2 - c_2, \cdots, x_n - c_n)$ 的理想. 这种形式理想一定是极大理想是很容易证的,然而另一方向的证明则需要 Hilbert 零点定理.

在第三章中我们曾看到在一些场合中素理想、极大理想的出现. 在这里,在环 $\mathbb{C}[x_1,\cdots,x_n]$ 中我们又在新的场合中看到它们. 这说明这些概念是重要的和有力的.

§4　Gröbner 基

在以下各节中我们介绍计算代数几何的一个基石:Gröbner 基理论.

在域 F 上一元多项式的理论中有重要的 Euclid 算法(对给定一元多项式 $f(x)$ 和 $g(x)$, 可按一定步骤计算出商式 $q(x)$ 和余式 $r(x)$),在域 F 上 n 元线性方程组的理论中有重要的 Gauss 算法(对给定方程组可按一定步骤计算或算出其解或得知它无解). 无论在理论上还是计算上它们起着巨大的作用. Euclid 算法可以说是关于环 $F[x]$ 的, Gauss 算法可以说是关于 F 上 n 维向量空间 F^n 的. 那么它们在 n 元多项式环 $F[x_1,\cdots,x_n]$ 中的相应物该是什么呢?

下面这个简单而要害的问题引发出计算代数几何:在域 F 上 n 元多项式环 $R = F[x_1,\cdots,x_n]$ 中给定 m 个多项式 $g_1,\cdots,g_m$, 以及 f, 求出一算法(即按一定规则进行的有限次计算程序)而能判断 f 是否属于理想 $(g_1,\cdots,g_m)$, 这就是说依据算法去计算,或者得出 R 中多项式 $q_1,\cdots,q_m$ 使 $f = q_1g_1 + \cdots + q_mg_m$, 或者得出结论: f 不可能表示成这种形式,就像 Gauss 算法之对于线性方程组那样.

对比一元多项式的 Euclid 算法，自然想到用 $g_1,\cdots,g_m$ 去除 f，即对多元多项式情况讨论“带余除法”. 我们就从这里入手.

“带余除法”的本质是用除式的首项去消被除式的首项，因而要对单项式引入一个序. $R = F[x_1,\cdots,x_n]$ 中的单项式集设为

$$S = \{x_1^{\alpha_1}\cdots x_n^{\alpha_n} = x^\alpha,\text{其中 } x = (x_1,\cdots,x_n),\alpha = (\alpha_1,\cdots,\alpha_n),\ \forall\ i,\alpha_i \in \mathbb{Z}^+ \cup \{0\}\},$$

设 $\{S,\leqslant\}$ 是一个序集，即 $\{S,\leqslant\}$ 是一个偏序集，且对任意 $x^\alpha,x^\beta \in S$，或 $x^\alpha \leqslant x^\beta$，或 $x^\beta \leqslant x^\alpha$，亦即 S 中任二元素都是可比的. 考虑到“带余除法”的需要，我们还要求 $\leqslant$ 满足下列条件:

(a) 若 $x^\alpha \leqslant x^\beta, x^\gamma \in S$，则有 $x^\alpha \cdot x^\gamma \leqslant x^\beta \cdot x^\gamma$;

(b) $\leqslant$ 是 S 的良序，即 S 的任意非空子集 M 总有最小元，即存在 $a \in M$ 使得对任意 $b \in M$ 有 $a \leqslant b$.

为确定计可取 S 的字典序:先规定 $x_1 > x_2 > \cdots > x_n$，然后对 S 中的两个单项式 x^α,x^β 按字典序排序，即当 $\alpha = (\alpha_1,\cdots,\alpha_n),\beta = (\beta_1,\cdots,\beta_n)$ 时规定 $x^\alpha > x^\beta$ 当且仅当 $\alpha_i = \beta_i, i = 1,2,\cdots,k-1$ 而 $\alpha_k > \beta_k$. 直接验证易知字典序符合上述(a),(b)两个条件.

这里我们立刻指出，和一元情况不同的是，当 $x^\beta < x^\alpha$ 时并不一定总有 $x^\beta | x^\alpha$，即 x^β 不一定能整除 x^α. 例如 $x_1^2x_2^3x_3x_4^5 < x_1^2x_2^3x_3^2x_4$，但 $x_1^2x_2^3x_3x_4^5 \nmid x_1^2x_2^3x_3^2x_4$. 另一方面，当 $x^\beta < x^\alpha$，肯定 $x^\alpha \nmid x^\beta$，这是和一元情况一样的.

除算法　在环 $R = F[x_1,\cdots,x_n]$ 中讨论，F 是域. 取定 S 的序 $\leqslant$.

(1) 用一个除式 g 去除 f 的程序:若 g 的首项 $LT(g)$ 不整除 f 的首项 $LT(f)$，则计算终止;若 $LT(f) = LT(g) \cdot a_1x^{\alpha_1}, a_1 \in F$，则令 $f_1 = f - a_1x^{\alpha_1} \cdot g, q_1 = a_1x^{\alpha_1}$，再对除式 g 去除 f_1，重复上面步骤，直至

$$q_t = a_1x^{\alpha_1} + \cdots + a_tx^{\alpha_t},\quad f_t = f - q_t \cdot g,$$

或 $f_t = 0$ 或 $LT(g) \nmid LT(f_t)$. 此时计算终止. 此时 $f = q_t \cdot g + r, LT(g) \nmid LT(r)$ 或 $r = 0$. 称 r 为 g 除 f 的余式.

(2) 用 m 个除式 $\{g_i, 1 \leqslant i \leqslant m\}$ 去除 f 的程序:先给定 m 个除式一个先后顺序，例如排列为 $g_1,g_2,\cdots,g_m$ (当然也可把 g_3 排在第一位). 依程序(1)用 g_1 去除 f，最终得 $f = q_{11} \cdot g_1 + r_{11}$;再用 g_2 去除 r_{11}，得 $r_{11} = q_{12} \cdot g_2 + r_{12}$ (随之，$f = q_{11} \cdot g_1 + q_{12} \cdot g_2 + r_{12}$)，这样继续下去，直至用 g_m 去除 $r_{1,m-1}$ 得 $r_{1,m-1} = q_{1m} \cdot g_m + r_{1m}$ (随之，$f = q_{11} \cdot g_1 + \cdots + q_{1m}g_m + r_{1m}$). 然后翻转回去再从 g_1 开始，用 g_1 去除 r_{1m}，如此反复下去，直至 $f = q_1g_1 + \cdots + q_mg_m + r$，且 $r = 0$ 或对任意 i，有 $LT(g_i) \nmid LT(r)$. 此时计算

终止.而称 r 为在给定序 $\leqslant$ 下,除式按 $g_1,\cdots,g_m$ 顺序排列去除 f 时得到的余式.

上面算法用计算机的程序语言可表达如下:

除算法程序 REDPOL

```
input: p_1,…,p_s,f
output|: a_1,…,a_s,g
a_1 := 0;…;a_s := 0;g := 0
c := f
begin
while  c ≠ 0   do
        i := 1
        divisionoccurred: = false
        while   i ≤ s   and  divisionoccurred = false  do
              if  LT(p_i) | LT(c)   then
                     a_i := a_i + LT(c)/LT(p_i)
                     c := c - (LT(c)/LT(p_i))p_i
                     divisionoccurred: = true
                     else  i: = i + 1
        if  divisionoccurred = false  then
             g := g + LT(c)
             c := c - LT(c)
end REDPOL
```

如果按除算法得到的余式 r 是"唯一"的,就好了.可惜这是不成立的.

例 在 $\mathbb{Q}[x,y]$ 中,$x>y$,取字典序.用 $g_1=xy+1,g_2=y^2-1$ 去除 $f=xy^2-x$.先按顺序 g_1,g_2 去除 f,依除算法得

$$f=y\cdot g_1+0\cdot g_2+(-x-y),$$

且 $LT(g_1)=xy\nmid -x=LT(-x-y),LT(g_2)=y^2\nmid -x=LT(-x-y)$.再按顺序 g_2,g_1 去除 f,依除算法得

$$f=x\cdot g_2+0\cdot g_1+0,r=0.$$

这说明除式的顺序在除算法中是影响最终结果的,同时也说明用 g_1,g_2 去除

f 时,是不唯一的,因而我们无法依余式 $r \neq 0$ 而去判断 f 不属于理想 (g_1, g_2).

为了判断是否 $f \in (g_1, \cdots, g_m)$ 而去用 $g_1, \cdots, g_m$ 去除 f, 这时我们还有一些有利条件可以利用:可以扩大除式队伍,在 $g_1, \cdots, g_m$ 上,再添加有限多个形如

$$h_1 \cdot g_1 + \cdots + h_m g_m \in (g_1, \cdots, g_m)$$

的除式,然后去除 f. 一方面用此扩大的除式集去除 f, 若得 $r = 0$, 仍知 $f \in (g_1, \cdots, g_m)$;另一方面,除式多,除式的首项也多,能够整除的单项式也多,能使除算法继续施行的机会也就多了,而有可能避免上例中的尴尬局面.

最理想的境界是在理想 $I = (g_1, \cdots, g_m)$ 中找到一组生成元 $h_1, \cdots, h_t$, 即 $I = (h_1, \cdots, h_t)$, 且 I 中任一多项式 g 的首项必被某一 h_i 的首项整除. 若是,当 $f \in I$ 时, 注意到依除算法用 $h_1, \cdots, h_t$ 去除 f 时在每一步骤中所得到的余式 r 也都属于 I, 因而除算法将永可执行直到最终 $r = 0$. 反之若 $f \notin I$, 则当然最终的余式 $r \neq 0$. 这样依除算法去计算,根据余式 r 是否为 0,就可判断是否 $f \in (h_1, \cdots, h_t)$.

定义 4.1 设 I 是域 F 上多项式环 $F[x_1, \cdots, x_n]$ 的非零理想,并取定单项式序 $\leqslant$. 若 $I = (g_1, \cdots, g_t)$ 且对任意 $f \in I$, 必有 i 使 $LT(g_i) \mid LT(f)$, 则称 I 的生成元集 $\{g_1, \cdots, g_t\}$ 为 I 的一个 Gröbner 基.

W. Gröbner 是奥地利代数几何专家,他对其学生 B. Buchberger 提出本节开始的那个简单而要害的问题,后者在 1965 年完成的博士论文中肯定地解决了它,而称之为 Gröbner 基以表对其老师的尊敬. 而早在 1962 年日本代数几何专家 H. Hironaka 也在发表的文章中提出这一概念,并称之为理想 I 的标准基,但只是在 Gröbner 基在计算代数界中引起广泛注意后,人们才发现日本人的工作.

如果回顾一下 Hilbert 基定理,特别是它的证明,我们不难在理论上说明理想的 Gröbner 基是存在的.

设 I 是环 $R = F[x_1, \cdots, x_n]$ 的一个非零理想. 令(对于取定的单项式序 $\leqslant$)

$$LT(I) = \{LT(f), f \in I\}.$$

它很像在证明 Hilbert 基定理时曾考虑过的一个理想. 然而现在的 $LT(I)$ 只是一些单项式的集合.

命题 4.2 $S \subseteq F[x_1, \cdots, x_n]$, S 是由一些单项式组成的集合. 则必有有限个单项式 $T_1, \cdots, T_t$ 使得 $(S) = (T_1, \cdots, T_t)$.

证明 注意到 (S) 是由一些单项式生成的理想,故 (S) 中每一多项式都是这些单项式的倍式的和,因而若 $f \in (S)$, 则多项式 f 的每一单项式也都

属于 (S).

由 Hilbert 基定理知,有 $f_1,\cdots,f_k \in (S)$ 使得 $(S)=(f_1,\cdots,f_k)$. 设这些多项式 $f_i, 1\leqslant i\leqslant k$, 中的所有的单项式为 $T_1,\cdots,T_t$, 则由上面的说明便得 $(S)=(T_1,\cdots,T_t)$. □

定理 4.3 $F[x_1,\cdots,x_n]$ 的每一理想 I 都有一个 Gröbner 基.

证明 考虑单项式集 $LT(I)$ 生成的理想 $(LT(I))$. 依上面命题有

$$(LT(I))=(T_1,\cdots,T_t), \tag{1}$$

其中这些 T_i 都是单项式. 注意到,一方面 T_i 必是单项式生成元集 $LT(I)$ 中某个单项式的倍式;另一方面,作为理想 I 中多项式的首项集, $LT(I)$ 是关于取单项式倍式封闭的,即若 $T\in LT(I)$, 则对任意单项式 M, $T\cdot M$ 也属于 $LT(I)$, 故有对每个 i, 有 $T_i\in LT(I)$. 随之依 $LT(I)$ 的定义,必有 $g_i\in I$ 使得 $LT(g_i)=T_i, 1\leqslant i\leqslant t$.

由(1)我们有,对任意 $T\in LT(I)$, 必有 i 使得 $T_i|T$, 亦即对任意 $f\in I$, 必有 i 使得 $T_i|LT(f)$.

这样 $g_i, 1\leqslant i\leqslant t$, 具有性质:

(i) $\{g_i, 1\leqslant i\leqslant t\}\subseteq I$;

(ii) 对任意 $f\in I$, 必有 i 使得 $LT(g_i)\,|\,LT(f)$.

为了证明 $g_i, 1\leqslant i\leqslant t$, 是理想 I 的 Gröbner 基,只需证 $I=(g_1,\cdots,g_t)$.

为此利用除算法,在取定的单项式序 $\leqslant$ 下,用 $g_1,\cdots,g_t$ 去除任意取定的 $f\in I$. 注意到 $g_1,\cdots,g_t$ 和 f 都在理想 I 中,因而用除算法所得到的余式 r 必也在理想 I 中. 由性质(ii),若 $r\neq 0$, 则必有 i, 使 $LT(g_i)\,|\,LT(r)$, 故除算法的计算终止时,必是 $r=0$. 随之 $f=q_1g_1+\cdots+q_tg_t$. 这就证明了 $I=(g_1,\cdots,g_t)$. □

从上面讨论中我们还得到 Gröbner 基的另两个彼此等价的定义:

定义 4.4 设 I 是 $F[x_1,\cdots,x_n]$ 的非零理想,取定单项式序 $\leqslant$. 若

1) $I=(g_1,\cdots,g_t)$ 且 $(LT(I))=(LT(g_1),\cdots,LT(g_t))$, 或

2) $\{g_1,\cdots,g_t\}\subseteq I$ 且 $(LT(I))=(LT(g_1),\cdots,LT(g_t))$,

则称 $\{g_1,\cdots,g_t\}$ 为理想 I 的一个 Gröbner 基.

显然理想 I 的 Gröbner 基不是唯一的,因为在 I 的一个 Gröbner 基上再添加 I 中有限多个元素,结果当然仍是 I 的一个 Gröbner 基. 为了节省计算时间,也为了在 I 的所有 Gröbner 基中选择一个最好的,我们引入下面

定义 4.5 设 $\{g_1,\cdots,g_t\}$ 是 $F[x_1,\cdots,x_n]$ 的理想 I 的一个 Gröbner 基,若它满足条件:

1) 所有 g_i 的首项系数都是 1;

2) 对任意 i, $LT(g_i) \notin (LT(g_j), j \neq i, 1 \leqslant j \leqslant t)$;

3) 对任意 i, g_i 中的任一单项式不被 $LT(g_j)$, $1 \leqslant j \leqslant t$, 整除.

就称 $\{g_1, \cdots, g_t\}$ 为 I 的一个简约 Gröbner 基.

从 I 的一个已知 Gröbner 基出发,不难把它改造成一个简约的. 1)是容易作到的,关于 2),如果, $LT(g_1) \in (LT(g_2), \cdots, LT(g_t))$, 则必有 $i \neq 1$, $LT(g_i) \mid LT(g_1)$ (这个事实我们在前面已用过了),这样,把 g_1 拿掉,仍有

$$(LT(g_2), \cdots, LT(g_t)) = (LT(g_1), LT(g_2), \cdots, LT(g_t)) = (LT(I)).$$

依定义 4.4,2)知 $\{g_2, \cdots, g_t\}$ 是 I 的 Gröbner 基. 所以在给定的 Gröbner 基中依上面方式把可以拿掉的都拿掉,就得到满足 2)者. 至于 3),如果,例如, g_1 的某一项(当然不是首项)被 $LT(g_2)$ 整除,则可用 g_2 消去 g_1 的这一项而得 $g_1 - qg_2$, 依定义 4.4,2)不难看出 $(g_1 - qg_2, g_2, \cdots, g_t)$ 仍是 I 的 Gröbner 基. 根据上面的说明,读者不难给出一个把已知的 Gröbner 基化成简约者的算法.

命题 4.6　理想 I 的简约 Gröbner 基是存在且唯一的.

证明　I 的 Gröbner 基是存在的(定理 4.3),因而上面的讨论说明简约 Gröbner 基也存在.

为了证明唯一性,设 $\{g_1, \cdots, g_t\}$ 和 $\{h_1, \cdots, h_s\}$ 都是 I 的简约 Gröbner 基. 由于 $g_1 \in I$, 故必有 j, 使 $LT(h_j) \mid LT(g_1)$. 同样,必有 i, 使 $LT(g_i) \mid LT(h_j)$. 随之有 $LT(g_i) \mid LT(g_1)$. 据简约性 1),2),由之便得 $g_1 = g_i$ 和 $LT(g_1) = LT(h_j)$. 这样继续作下去,并对 h_j 重新编号,可得 $t = s$ 且 $LT(g_i) = LT(h_i)$, $1 \leqslant i \leqslant t$. 今考察 $g_1 - h_1 \in I$, g_1, h_1 的首项相同而被消去. 而依简约性 3), g_1, h_1 的其它项都不被 $LT(g_i) = LT(h_i)$ 整除, $i = 1, 2, \cdots, t$. 随之若 $g_1 - h_1 \neq 0$, 则 $g_1 - h_1$ 的首项也必不被 $LT(g_i) = LT(h_i)$ 整除, $i = 1, 2, \cdots, t$. 这和 $\{g_i, 1 \leqslant i \leqslant t\}$, $\{h_j, 1 \leqslant j \leqslant s = t\}$ 是 Gröbner 基矛盾. 故必 $g_1 = h_1$. 同理对每个 i, 有 $g_i = h_i$. □

在用简约 Gröbner 基 $g_1, \cdots, g_t$ 去除 f 时,我们也可对余式 r 提出类似上面简约性(3)的要求:余式 r 中的每一项都不被 $LT(g_i)$ 整除, $i = 1, 2, \cdots, t$. 这时我们便有了余式的唯一性.

命题 4.7　$\{g_1, \cdots, g_t\}$ 是理想 I 的简约 Gröbner 基, $f \in F[x_1, \cdots, x_n]$. 若

$$f = q_1 g_1 + \cdots + q_t g_t + r,$$

$$f = q'_1 g_1 + \cdots + q'_t g_t + r',$$

其中 r 和 r' 中的每一项都不被 $LT(g_i)$ 整除, $i = 1, 2, \cdots, t$, 则 $r = r'$. □

需要提一下的是,这里我们不能指望商式 q_i, $1 \leqslant i \leqslant t$, 的唯一性.

再总结一下：我们选定单项式序 $\leqslant$ 后，如果能对给定的理想 I 具体找出它的简约 Gröbner 基，则随意排定除式顺序后，依除算法，就能判断 f 是否在 I 中：余式 $r=0$，则 $f\in I$，余式 $r\neq 0$，则 $f\notin I$.

应该说，只是当除式集是一个 Gröbner 基，除算法才是有力工具.

这里的一切算法，概念都是在选定的单项式序 $\leqslant$ 下进行的.不同的序对计算的快慢和计算的结果都有本质的影响.对此本书中将不作进一步分析.只限于再介绍几种可用的单项式序.设 $S=\{x^{\alpha},\alpha=(\alpha_1,\cdots,\alpha_n),\alpha_i\in\mathbb{Z}^+\cup\{0\}\}$ 规定 $|\alpha|=\sum\limits_{1}^{n}\alpha_i$.

S 的分次字典序　$x^{\alpha}>x^{\beta}$，若 $|\alpha|>|\beta|$，或 $|\alpha|=|\beta|$ 时依字典序 $\alpha>\beta$.

S 的分次反字典序　$x^{\alpha}>x^{\beta}$，若 $|\alpha|>|\beta|$ 或 $|\alpha|=|\beta|$ 时 $\alpha-\beta=(\alpha_1-\beta_1,\cdots,\alpha_n-\beta_n)$ 最右非 0 数是负的.

§5　Buchberger 算法

本节将给出由 $F[x_1,\cdots,x_n]$ 的理想 I 的一个给定生成元系 $\{g_1,\cdots,g_s\}$ 去计算 I 的一个 Gröbner 基的算法.

理想 I 的一个生成元系 $G=\{g_1,\cdots,g_s\}$ 和 I 的一个 Gröbner 基的差距就在于后者提供"完备"的首项 $LT(h_i),1\leqslant i\leqslant t$，亦即 $(LT(h_i),1\leqslant i\leqslant t)=(LT(I))$. 因而把生成元系 $G=\{g_1,\cdots,g_m\}$ 扩大成为一个 Gröbner 基的一个自然想法，就是对它添加能提供新首项的 I 中元素(亦即形如 $q_1g_1+\cdots+q_sg_s$ 的元素)，而从 G 中任二元素 g_i,g_j 消去首项而得到者该是获得这样多项式的最简单的方法.

由于 F 是域，不失一般性，不妨设 g_i 的首项系数都是 1.

设 $LT(g_i)=x^{\alpha},LT(g_j)=x^{\beta}$，单项式 x^{α},x^{β} 的最小公倍式为 $x^{\gamma}=x^{\alpha}x^{\alpha'}=x^{\beta}x^{\beta'}$，其中 $\gamma=(\gamma_1,\cdots,\gamma_n),\gamma_i=\max(\alpha_i,\beta_i),\alpha'=\gamma-\alpha=(\gamma_1-\alpha_1,\cdots,\gamma_n-\alpha_n),\beta'=\gamma-\beta=(\gamma_1-\beta_1,\cdots,\gamma_n-\beta_n)$. 为了消去 g_i,g_j 的首项，最经济的方法就是考虑

$$S(g_i,g_j)=x^{\alpha'}g_i-x^{\beta'}g_j.$$

这里顺便该提到的，如果不用最经济的方法，即考虑 $m_ig_i-m_jg_j$，其中 m_i,m_j 是单项式，有 $LT(m_ig_i)=LT(m_jg_j)\geqslant x^{\gamma}$，因而仍能彼此消去首项，此时当然 $m_ig_i-m_jg_j=m'S(g_i,g_j)$，其中 m' 是单项式，而 $LT(m'S(g_i,g_j))<LT(m_ig_i)=LT(m_jg_j)$.

约定:虽然单项式序 $\leqslant$ 只是定义在单项式集上,为了方便,也可扩大到带非 0 系数 $c \in F$ 的单项式,而规定,若 $x^{\alpha} \leqslant x^{\beta}$, 我们也说 $cx^{\alpha} \leqslant dx^{\beta}$, c, d 为 F 中非 0 元素.

上面这个特殊的由 g_i, g_j 消去首项而得的 $S(g_i, g_j)$ 的方法也蕴含了由 $g_1, \cdots, g_m$ 消去首项而获得新多项式的一般方法,即有

命题 5.1 设 $g_i, 1 \leqslant i \leqslant s$, 的首项系数都是 1. $m_i = x^{\alpha(i)}$ 是系数为 1 的单项式,且对每个 i, 有 $LT(m_i g_i) = x^{\delta}$. 若 $f = \sum_{1}^{s-1} c_i m_i g_i$, 其中对每个 i, 有 $c_i \in F$, $LT(f) < x^{\delta}$, 则

$$f = \sum_{1}^{s-1} d_i m'_i S(g_i, g_{i+1}).$$

其中对每个 i, 有 $LT(d_i m'_i S(g_i, g_{i+1})) < x^{\delta}$, $d_i \in F$ 且 m'_i 是系数为 1 的单项式.

证明 由假设 $LT(m_i g_i) = x^{\delta}$ 而 $LT(f) < x^{\delta}$ 知,在和 $\sum c_i m_i g_i$ 中所有 $c_i m_i g_i$ 的首项($= c_i x^{\delta}$)是彼此消去的,故必 $c_1 + c_2 + \cdots + c_s = 0$. 再注意到命题前的说明,我们有

$$\begin{aligned} f = \sum_{s}^{1} c_i m_i g_i &= c_1(m_1 g_1 - m_2 g_2) + (c_1 + c_2)(m_2 g_2 - m_3 g_3) \\ &\quad + \cdots + (c_1 + \cdots + c_{s-1})(m_{s-1} g_{s-1} - m_s g_s) + (c_1 + \cdots + c_s) m_s g_s \\ &= d_1 m'_1 S(g_1, g_2) + d_2 m'_2 S(g_2, g_3) + \cdots + d_{s-1} m'_{s-1} S(g_{s-1}, g_s). \end{aligned}$$

其中 $d_i = c_1 + c_2 + \cdots + c_i \in F$, m'_i 是单项式,且对每个 i, 有

$$LT(d_i m'_i S(g_i, g_{i+1})) < LT(f) = x^{\delta}. \qquad \square$$

将把依除算法用 $g_1, \cdots, g_t$ 去除 f 所得余式 r 记作 $r(f \mid g_1, \cdots, g_t)$. 下面定理给出理想 I 的一个生成元系是一个 Gröbner 基的判断准则.

定理 5.2 $G = \{g_1, \cdots, g_t\} \subseteq F[x_1, \cdots, x_n]$, 取定单项式序 $\leqslant$. 则 G 是 $I = (G)$ 的一个 Gröbner 基当且仅当对任意 i, j, 有

$$r(S(g_i, g_j) \mid g_1, \cdots, g_t) = 0. \qquad (*)$$

证明 若 G 是 I 的 Gröbner 基,由于 $S(g_i, g_j)$ 是 g_i, g_j 的线性和,随之属于 I, 故由 Gröbner 基的性质及除算法,即得 (*) 成立.

今设 (*) 成立,往证 $\{g_1, \cdots, g_t\}$ 是 I 的 Gröbner 基.

(*) 的意义是,依除算法用 $g_1, \cdots, g_t$ 去除 $S(g_i, g_j)$ 时余式为零. 注意到在除算法的过程中,商式和除式乘积的首项永远不会大于被除式的首项,故 (*) 成立意味着有

$$S(g_i, g_j) = \sum_{k=1}^{t} q_{ijk} g_k, \qquad (1)$$

且满足性质(P):对任意 i,j,k,有

$$LT(q_{ijk}g_k) \leqslant LT(S(g_i,g_j)).$$

值得强调一下的是,既然 $S(g_i,g_j) \in I$,永远有(1),但能有性质(P)却是(∗)成立的结果.

下面用反证法来证.设存在 $f \in I$,有(B):$LT(f) \notin (LT(g_i) \mid 1 \leqslant i \leqslant t)$.

由 $f \in I = (g_1,\cdots,g_t)$,则 f 可表成 g_i 的线性和,可以有许多不同表达式,取其一,设为 $f = \sum_i c_i h_i g_i, c_i \in F$,而认定多项式 h_i, g_i 的首项系数都是 1.设 $LT(h_i g_i), 1 \leqslant i \leqslant t$,中之最大者为 x^δ.此时必有 $LT(f) < x^\delta$,否则与(P)矛盾.多项式 f 的每一表达式都如上对应一个单项式,这些单项式中必有最小者(根据单项式序 $\leqslant$ 的性质(b)),不妨就设为 x^δ.下面将利用(∗)而得 f 的另一表达式,它对应的单项式 $x^\alpha < x^\delta$,因而得出矛盾.

适当重新编号可认定 $LT(h_i g_i) = x^\delta, 1 \leqslant i \leqslant s, LT(h_j g_j) < x^\delta, s+1 \leqslant j \leqslant t$.令 $LT(h_i) = m_i, 1 \leqslant i \leqslant s$,今计算

$$\begin{aligned} f &= \sum\nolimits_1^t c_i h_i g_i = \sum\nolimits_1^s c_i h_i g_i + \Big(\Big[\sum\nolimits_{s+1}^t c_j h_j g_j\Big)\Big]_1 \\ &= \sum\nolimits_1^s c_i m_i g_i + \Big(\Big[\sum\nolimits_1^s c_i(h_i - m_i)g_i + \sum\nolimits_{s+1}^t c_j h_j g_j\Big)\Big]_2. \end{aligned}$$

根据前面命题 5.1 以及(1),我们有

$$\begin{aligned} \sum\nolimits_1^s c_i m_i g_i &= \sum\nolimits_1^{s-1} d_i m'_i S(g_i, g_{i+1}) = \sum\nolimits_1^{s-1} d_i m'_i \sum\nolimits_1^t q_{i,i+1,k} g_k \\ &= \Big(\Big[\sum\nolimits_1^{s-1} \sum\nolimits_1^t d_i m'_i q_{i,i+1,k} g_k\Big)\Big]_3. \end{aligned}$$

显然方括号$[\quad]_1$,$[\quad]_2$中每一项都小于 x^δ.$[\quad]_3$中的每一项也都小于 x^δ,这是因为,利用性质(P),

$$LT(m'_i q_{i,i+1,k} g_k) \leqslant LT(m'_i S(g_i, g_{i+1})) < LT(m_i g_i) = x^\delta.$$

再注意到 $f = [\quad]_3 + [\quad]_2$,这样便得 f 的一个表成 $g_1,\cdots,g_t$ 线性和的表达式,而此表达式中的每一项都小于 x^δ,这和 x^δ 的选择是矛盾的,因而对任意 $f \in I$,都有 $LT(f) \in (LT(g_i) \mid 1 \leqslant i \leqslant t)$,即 $\{g_1,\cdots,g_t\}$ 是 $I = (g_1,\cdots,g_t)$ 的 Gröbner 基.□

这个定理是说,如果 $S(g_i,g_j)$ 提供不出新的首项的话,那么 $G = \{g_1,\cdots,g_t\}$ 就是 $I = (g_1,\cdots,g_t)$ 的 Gröbner 基.这个结论是有力的,它将给出一个计算 Gröbner 基的算法.这个结论也是意料中的:读者该会有同感的,想从这些 g_i 得有新首项的多项式,自然会想到 $S(g_i,g_j)$,因而考虑说明 $S(g_i,g_j)$ 的一般地位的命题 5.1,有了命题 5.1,那么定理 5.2 就是一个可作为猜想的

命题了.上定理的证明是初等的,简单的,也是很巧妙的.

由给定的 $G = \{g_1, \cdots, g_m\} \subseteq F[x_1, \cdots, x_n]$,取定的单项式序 $\leqslant$,可如下去计算 $I = (g_1, \cdots, g_m)$ 的一个 Gröbner 基:把不等于零的 $r(S(g, g') | G)$, $g, g' \in G$ 都添加到 G 集中,得

$$G \cup \{r(S(g, g') | G) \neq 0 | g, g' \in G\},$$

把此扩大了的 G 集,仍记作 G 而重复上面步骤.最后达到一个比最初的 $G = \{g_1, \cdots, g_m\}$ 扩大了的 $G_1 = \{g_1, \cdots, g_m, \cdots, g_t\}$,而对这个 G_1 言 $r(S(g_i, g_j) | g_1, \cdots, g_t) = 0$ 对任意 i, j 成立,这时依上面定理,G_1 就是理想

$$I = (G_1) = (G) = (g_1, \cdots, g_m)$$

的一个 Gröbner 基.

用程序化语言可叙述如下:

Input: $F = (f_1, \cdots, f_s)$

Output: a Gröbner basis $G = \{g_1, \cdots, g_t\}$ for

$I = (F)$ with $F \subseteq G$

Repeat

$G' := G$

For each pair $\{p, q\}$, $p \neq q$ in G' Do

$r := r(S(p, q) | G')$

If $r \neq 0$ Then $G := G \cup \{r\}$

Until $G = G'$

从理论上讲上述算法中的迭代过程应在有限步停下来,因为当 $G' \subsetneq G$ 时

$$(LT(g), g \in G') \subsetneq (LT(g), g \in G),$$

而依 Hilbert 基定理,这个重复过程不能无穷地继续下去.

这个算法(以及改进的算法,以使计算更快更好)在文献中被称作 Buchberger 算法.除算法,以及 Buchberger 算法合在一起就完全解决了给定的多项式 f 是否属于给定理想 $I = (g_1, \cdots, g_m)$ 的问题.它是计算代数几何的一个基石.在一些软件如 Mathematica, Maculay 等中都有专门设计好的程序实现这个算法,因而计算 Gröbner 基是方便和容易的.当然也有发生长时间计算而计算机给不出结果的情形.虽然原则上应"在有限步上停下来",但时间过长,计算机存储小,在"实际上"也有时是不能实现的.

在有关代数几何的一些计算或理论问题上,Gröbner 基都显示它的力量.在本节最后,作为例子,我们回到本章开始解高次代数方程组问题.

在 $\mathbb{C}[x_1, \cdots, x_n]$ 中考虑联立方程组

$$\begin{cases} f_1(x_1,\cdots,x_n)=0, \\ \quad\vdots \\ f_m(x_1,\cdots,x_n)=0. \end{cases} \tag{2}$$

我们拟用消元法来求解,即在 $g_1f_1+\cdots+g_mf_m$ 中找出含未知量尽可能少的多项式来.设理想 $I=(f_1,\cdots,f_m)$.令 $I_k=I\cap\mathbb{C}[x_{k+1},\cdots,x_n]$.易知 I_k 是环 $\mathbb{C}[x_{k+1},\cdots,x_n]$ 的理想,I_k 是由 I 中一切不含变元 $x_1,\cdots,x_k$ 的多项式组成的.称 I_k 为 I 的 k 次消去理想.例如,如果我们找到 I_{n-1} 中的元素,那就是说在形如 $g_1f_1+\cdots+g_mf_m$ 中找到一个只含 x_n 的多项式.

定理 5.3 (消去定理) I 是 $A=F[x_1,\cdots,x_m]$ 的理想,把单项式序 $\leqslant$ 取作字典序而令 $x_1>x_2>\cdots>x_n$.设 $G=\{g_1,\cdots,g_t\}$ 是 I 的一个 Gröbner 基.令环 $A_k=F[x_{k+1},\cdots,x_n]$, $I_k=I\cap A_k$, $G_k=G\cap A_k$.则 $I_k=(G_k)$ 且 G_k 是环 A_k 中理想 I_k 的一个 Gröbner 基, $1\leqslant k\leqslant n-1$.

证明 为直观计,我们来证明 $k=2$ 的情况.欲证 $I_2=(G_2)$,只需证明任意 $f\in I_2$ 必有 $LT(f)\in(LT(g),g\in G_2)$.由于 G 是 I 的 Gröbner 基,而 $f\in I_2\subseteq I$,故有 $LT(f)\in(LT(g),g\in G)$,即 $LT(f)$ 是某个 $g\in G$ 的首项 $LT(g)$ 的倍式.另一方面,由字典序以及 G_k 的定义知

$$G=(G\setminus G_1)\cup(G_1\setminus G_2)\cup G_2,$$

其中 $G\setminus G_1$(可能是空集)中的多项式的首项必含 x_1, $G_1\setminus G_2$(可能是空集)中的多项式的首项不含 x_1 但必含 x_2.又注意到 $f\in I_2$,$LT(f)$ 不含 x_1 和 x_2,合起来便得 $LT(f)$ 只能是 G_2 中某个多项式 g 的 $LT(g)$ 的倍式,亦即 $LT(f)\in(LT(g),g\in G_2)$.依 Gröbner 基定义知 G_2 是 I_2 的 Gröbner 基,当然也有 $I_2=(G_2)$. □

如果把这个定理应用到解方程组(2),那就是:把多项式 $f_1,\cdots,f_m$ 输入计算机,然后屏幕上显示理想 $(f_1,\cdots,f_m)$ 的一个既约 Gröbner 基.如果用这些 f_i 真能消去变元 $x_1,\cdots,x_k$ 的话,你就能从这个 Gröbner 基读到,并且它们生成一切可能的这些不含 $x_1,\cdots,x_k$ 的多项式,也就是说一个都不会漏掉.用下面两个例子结束本节.

例 1 解高次代数方程组

$$\begin{cases} x^2+y+z=1, \\ x+y^2+z=1, \\ x+y+z^2=1. \end{cases}$$

在环 $\mathbb{C}[x,y,z]$ 中,令 $x>y>z$ 而取字典序 $\leqslant$.令

$$I=(x^2+y+z-1,x+y^2+z-1,x+y+z^2-1),$$

计算机给出 I 的既约 Gröbner 基:

$$g_1 = x + y + z^2 - 1,$$
$$g_2 = y^2 - y - z^2 + z,$$
$$g_3 = 2yz^2 + z^4 - z^2,$$
$$g_4 = z^6 - 4z^4 + 4z^3 - z^2.$$

由 $g_4 = z^2(z-1)^2(z^2+2z-1)$ 得 g_4 的根为 $z = 0, 1, -1 \pm \sqrt{2}$.

将 z 值代入 g_2, g_3 而得相应的 y 值,再把 z, y 值代入 g_1 可得相应的 x 值.最后代入方程组检验后得到下面 5 个解:

$$(1,0,0),(0,1,0),(0,0,1),(-1+\sqrt{2},-1+\sqrt{2},-1+\sqrt{2}),$$
$$(-1-\sqrt{2},-1-\sqrt{2},-1-\sqrt{2}).$$

例 2　解线性方程组

$$\begin{cases} x - 2y - z - w = 0, \\ 3x - 6y - 2z = 0, \\ 2x - 4y + 4w = 0. \end{cases}$$

在环 $\mathbb{C}[x,y,z,w]$ 中,令 $x > y > z > w$ 而取字典序 $\leqslant$. 令

$$I = (x - 2y - z - w, 3x - 6y - 2z, 2x - 4y + 4w),$$

得 I 的一个 Gröbner 基: $x - 2y - z - w, z + 3w$ 及 I 的一个既约 Gröbner 基: $x - 2y + 2w, z + 3w$. 把它们写成矩阵形式便是

$$\begin{pmatrix} 1 & -2 & -1 & -1 \\ 3 & -6 & -2 & 0 \\ 2 & -4 & 0 & 4 \end{pmatrix}, \quad \begin{pmatrix} 1 & -2 & -1 & -1 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & -2 & 0 & 2 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

1. 方程组　　　　2. I 的 Gröbner 基　　　　3. I 的既约 Gröbner 基

如果用 Gauss 消去法解这个方程组,则其正过程给出矩阵 2,而全(正反)过程给出矩阵 3. 从这里看到 Buchberger 算法是 Gauss 算法的一个推广.

§6　初等几何的机器证明

我们处在计算机时代.在学习和研究数学时,除了一支笔一张纸外,如何使用计算机这个有力工具,是自然要考虑到的一个问题.这一节中介绍的初等几何的机器证明是这一方面的重要成果.这个问题由 Descartes 和 Hilbert 开始,而由我国数学家吴文俊在 20 世纪 70 年代把它推向高峰的.

在这里坐标化再一次显示其威力. Descartes 引入坐标系把几何和代数密切的联系起来.我们想再一次强调的是:除了 Descartes 的坐标化,在前面已多次运用(广义)坐标化思想去把不同性质的对象联系起来,如对称与群,多项式

与其分裂域，多项式的分裂域与其 Galois 群，代数簇与理想等等，并初步看到用群刻画对称，用分裂域去刻画多项式的根，用 Galois 群去研究分裂域，用理想去研究代数簇的力量.

下面就在我们熟悉的(直观)平面几何及其解析几何的基础上，来讨论初等平面几何的机器证明，基本思路是：

(1) 把平面几何问题(定理)的“已知”和“求证”在某一坐标系下都翻译成为代数(多项式)关系式；

(2) 探讨这些“已知”中的代数关系式与“求证”中的代数关系式之间的因果联系而得出结论，这一工作应能由计算机完成.

(3) 将此代数结论翻译成几何结论.

(1)，(2)，(3)的意义，通过下面两个例子就可看清楚了.

例 1　Desargues 定理. 如图 1. 已知：$A'B' \parallel AB$，$A'C' \parallel AC$，$B'C' \parallel BC$，BB' 和 AA' 相交于 O；求证：O 在 CC' 上.

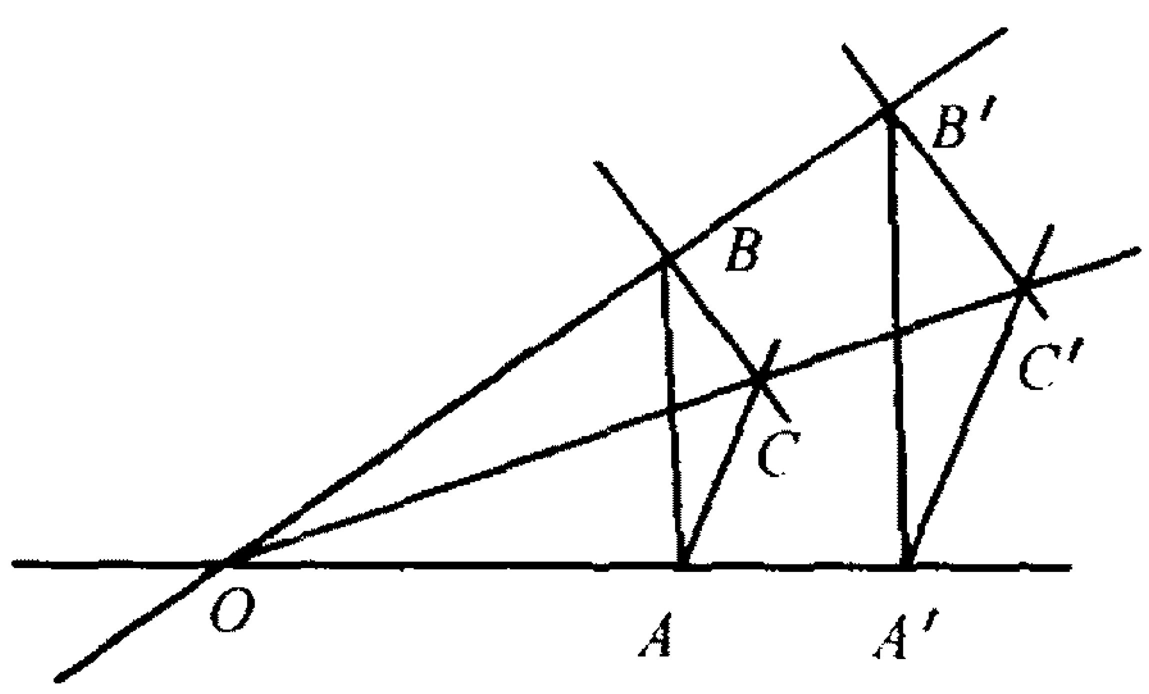


图 1

引入(仿射)坐标系如图 1，则可设各点的坐标如下：

$$A=(u_1,0);\qquad A'=(u_2,0);$$
$$B=(0,u_3);\qquad C=(u_4,u_5);$$
$$B'=(0,x_1);\qquad C'=(x_2,x_3).$$

这里 $u_i, i=1,2,3,4,5$，是独立参数，而 $x_i, i=1,2,3$，则可依已知条件而由诸 u_i 确定. 这也就是说 A,B,C,A' 诸点，依题意，是可以随意选定的，而 B',C' 两点，依题意，是随 A,B,C,A' 诸点选定而确定的.

现在把几何条件翻译成代数关系式.

已知：

$A'B' \parallel AB \Longleftrightarrow u_1x_1-u_2u_3=0$；

$A'C' \parallel AC \Longleftrightarrow (u_4-u_1)x_3-u_5(x_2-u_2)=0$；

$B'C' \parallel BC \Longleftrightarrow u_4(x_3-x_1)-(u_5-u_3)x_2=0$；

A,B,C 三点不共线 $\Longleftrightarrow -u_1u_5+u_1u_3-u_4u_3+1=0$，

求证：O 在 CC' 上 $\Longleftrightarrow u_4x_3 - u_5x_2 = 0$.

上面我们在已知条件中写进“A,B,C 三点不共线”，这一点很重要，因为在退化情形，即 A,B,C 三点共线时，Desargues 定理是可以不成立的.

在多项式环 $\mathbb{R}[u_1,u_2,u_3,u_4,u_5,x_1,x_2,x_3]$ 中，令

$f_1 = u_1x_1 - u_2u_3,\quad f_2 = (u_4 - u_1)x_3 - u_5(x_2 - u_2),$

$f_3 = u_4(x_3 - x_1) - (u_5 - u_3)x_2,\quad f_4 = - u_1u_5 + u_1u_3 - u_4u_3 + 1,$

$g = u_4x_3 - u_5x_2.$

这样 Desargues 定理的代数形式就是：若

$$(u_1,u_2,u_3,u_4,u_5,x_1,x_2,x_3) = (a_1,a_2,a_3,a_4,a_5,b_1,b_2,b_3)$$

是方程组

$$f_i = 0,\ i = 1,2,3,4$$

的任意一个实数解时，则此解也必使 $g = 0$. 这是因为，利用这个实数解，按照上面几何－代数的对应法则，可得一如图 1 中的几何图形. 而此时“此解也满足 $g = 0$”的几何意义即是 O 在 CC' 上. 这就是说，欲证几何中的 Desargues 定理，只需证明多项式 g 属于理想 (f_1,f_2,f_3,f_4)，而根据 Gröbner 基理论，这一工作是完全可以由计算机完成的.

下面是用 Maple 软件计算时，在荧屏上显示的内容：

```
> with(grobner);
  [finduni, finite, gbasis, gsolve, leadmon, normalf, solvable,
  spoly]
> F: = [u1 * x1 - u2 * u3,(u4 - u1) * x3 - u5 * (x2 - u2),u4 * (x3 - x1)
      - (u5 - u3) * x2,1 - u1 * u5 + u1 * u3 - u4 * u3];
  F: = [u1 x1 - u2 u3,(u4 - u1) x3 - u5 (x2 - u2),
      u4 (x3 - x1) - (u5 - u3) x2,1 - u1 u5 + u1 u3 - u4 u3]
> X: = [x1,x2,x3,u1,u2,u3,u4,u5];
  X: = [x1,x2,x3,u1,u2,u3,u4,u5]
> G: = gbasis(F,X);
  G: = [u1 x1 - u2 u3,1 - u1 u5 + u1 u3 - u4 u3,x2 u3 - u4 x1,
      x3 u4 - u5 x2,

                                       2
  x3 u1 - u5 u2 - u5 u4 x1 - u5 u2 + x3 + u3 u5 u2,
    2
  - u4 x1 - u4 u5 u2 + u4 u2 u3 + x2,
    2     2     2     2
```

```
x3 u5 u2 - x3 + x1 u5 x2 - x1 u5 u2,
                              2
x2 u5 u4 x1 - u5 u2 u4 x1 + u5 u2 x2 - x2 x3,
  2                        2
u2 u3 - x1 u4 u3 - u5 u4 x1 - u5 u2 + x3 + x1, - u4 u2 + x2 u1,
                   2         2          2
x3 u3 - x1 u5,x2 u4 x1 - u4 u2 x1 + u4 u2 u5 x2 - x2 ]
> normalf(u4 * x3 - u5 * x2,G,X);
                              0
```

其中以 > 起的行是输入，其它行是计算机的输出. gbasis(F, X)是求理想 $I = (f_1, f_2, f_3, f_4)$ 的 Gröbner 基，normalf 是用 I 的 Gröbner 基去除 g，下面的"0"说明余式为 0，即 $g \in I$，因而定理得证.

这样，对于几何中的所有"等式"命题，即在已知和求证中不出现大于或小于关系时，都可纳入下面一般解法中：在引入坐标系后给定几何命题的已知相当于 $f_i = 0, f_i \in \mathbb{R}[u_1, \cdots, u_n], i = 1, \cdots, m$；给定几何命题的求证相当于 $g = 0$（如果求证多个结论，则可分解为若干单一结论的命题）. 以上工作要我们来做. 然后交给计算机去验证 g 是否属于理想 $I = (f_i, i = 1, \cdots, m)$. 虽然，不属于时，我们尚不好完全肯定该几何命题不成立（这一方面我们不去进一步讨论）. 但当 g 属于理想 I，则肯定该几何命题是成立的. 在这里，我们是采用 Gröbner 基理论中的 Buchbager 算法来解决"方程组 $f_i = 0, 1 \leqslant i \leqslant m$，的实数解必是 $g = 0$ 的解"这一代数问题. 吴文俊对这一代数问题给出吴法（也称 Ritt－吴法），它更适用于由几何问题引出的方程组 $f_i = 0, 1 \leqslant i \leqslant n$，而常能更有效. 吴法把一度冷落的几何定理机器证明推向高峰. 周咸青用吴法证明了 512 个非平凡定理，且其中许多是新发现的. 我国在几何定理机器证明方面处于国际领先地位. 有兴趣的读者请参看相应的参考书.

我们用下面的例子结束本节.

垂心定理　任意三角形的三个垂线交于一点. 如图 2，引入直角坐标系，则已知：

$AD \perp BC \Longleftrightarrow f_1 \equiv y_3 y_5 - y_2(y_4 - y_1) = 0$；

$BD \perp AC \Longleftrightarrow f_2 \equiv y_3 y_5 - y_1(y_4 - y_2) = 0$；

A, B, C 不共线 $\Longleftrightarrow f_3 \equiv (y_2 - y_1) y_3 - 1 = 0$，

求证：CO 过 D 点 $\Longleftrightarrow g \equiv y_4 = 0$.

用 Maple 软件计算结果如下：

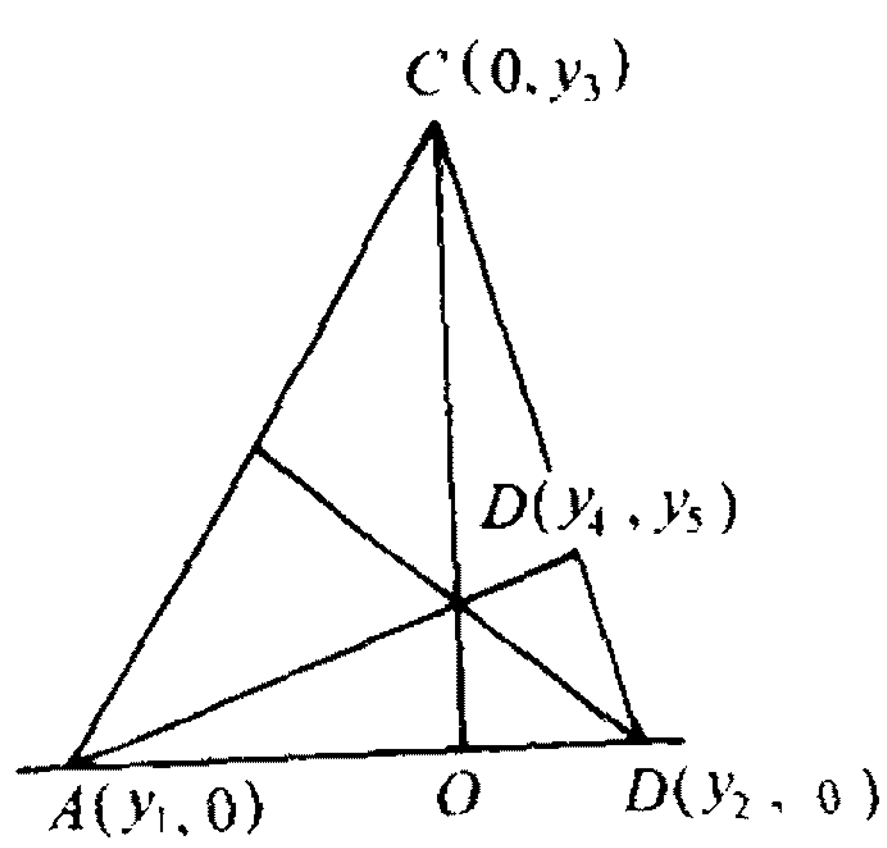


图 2

```
> Y: = [y1,y2,y3,y4,y5];
```

```
          Y := [y1,y2,y3,y4,y5]
> K:=[y3*y5-y2*(y4-y1),y3*y5-y1*(y4-y2),(y2-y1)*y3
     -1];
   K:=[y3 y5 - y2 (y4 - y1),y3 y5 - y1 (y4 - y2),
      (y2 - y1) y3 - 1]
> H:=gbasis(K,Y);
                 2           2
   H := [y3 y2 + y3 y5 - y2,y3 y5 + y2 y1,y4,
               - y3 y2 + y3 y1 + 1]
> normalf(y4,H,Y);
                           0
```

定理证完.

参考书目

1. 张禾瑞．近世代数基础(1978 年修订本)．北京:人民教育出版社,1978

2. 吴文俊．几何定理机器证明的基本原理(初等几何部分)．北京:科学出版社,1984

3. 熊全淹．近世代数．武汉:武汉大学出版社,1984

4. 聂灵沼,丁石孙．代数学引论．北京:高等教育出版社,1988

5. 潘承洞,潘承彪．初等代数数论．山东:山东大学出版社,1991

6. 万哲先．代数和编码(修订版)．北京:科学出版社,1980

7. Shafarevich I R Basic Notions of Algebra, Encyclopaedia of Mathematical Sciences. Berlin: Springer-Verlag, 1990

8. Artin M. Algebra. Englewood Cliffs: Prentice-Hall, 1991

9. Nikulin V V, Shafarevich I R. Geometries and Groups. Beijing: Springer-Verlag, World Publishing Corporation, 1989

10. Cox D, Little J, O'Shea D. Ideals, Vareties and Algorithms——An Introduction to Computational Algebraic Geometry and Commutative Algebra. New York: Springer-Verlag, 1992

11. Kendig K. Elementary Algebraic Geometry. Beijing: Springer-Verlag, World Publishing Corporation, 1977

符 号 表

$\mathbb{Z}$　整数环

$\mathbb{Q}$　有理数域

$\mathbb{R}$　实数域

$\mathbb{C}$　复数域

$\mathbb{Z}_p$　p 元域

$\mathrm{Aut}(G)$　群 G 的自同构群

$\mathrm{End}\ M$　加群 M 的自同态环

$\mathrm{Im}\ \phi$　同态 ϕ 的象

$\mathrm{Ker}\phi$　同态 ϕ 的核

$[K:F]$　F－向量空间 K 的维数,其中 $F\subseteq K$,F,K 是域

$\mathrm{Gal}(K/F)$　正规扩域 K 在 F 上的 Galois 群

$\mathrm{Inv}\ H$　群 H 作用下的不变子域

名词索引

A-模　51,121
Abel 群　13
Buchberger 算法　188
Burnside 问题　64
Cardana-Tartaglia 公式　158
Cayley 表　7
Cayley 定理　31
Chasles 定理　2
Cauchy 序列　86
Euclid 带余除法　106
Euclid 环　73
F - 次数　126
F - 共轭　138
F - 同构　133
Frobenius 定理　90
Galois 对应　144
Galois 基本定理　145,146
Galois 群　10,141
Galois 域　136
Gauss 环　111
Gauss 引理　114
Gröbner 基　182
G - 轨道　68
G - 集　66
Hamming 码　168
Hamming 距离　163
Hilbert 零点定理　172
Hilbert 基定理　173
I - 进 Cauchy 序列　87
I - 进完备环　87
Jordan 标准型　70
Klein 四元群　91
Lagrange 定理　42
Lie 型单群　54
n 元对称群　9
n 阶自由交换群　60
Noether 环　173
p - 群　45
p - 进整数环　88
Pythagoras 扩域　155
Sylow - 子群　45
Sylow 定理　45
Sylvester 指标定理　70
V - 理想　171
Wedderburn 定理　137
X - 字　60
Zorn 引理　103

（以下按汉语拼音字母次序排列）

B

半群　12
半群代数　97
本原多项式　113
毕氏扩域　155
变换　1
　一一变换　1
变换群　3
不定元　94
不可约簇　176

不可约多项式 106
不可约理想 176

C

超越扩域 127
超越数 127
超越元 127
传递 G-集 68
除环 137
除算法 180
簇 170
簇分解的存在性定理 177
簇分解的唯一性定理 177

D

代数 90
代数闭域 138
代数的表示 121
代数扩域 127
代数数 127
代数元 127
单扩域 126
单同态 38,78
单位 107
单位元 73
导式 128
等价关系 33
对称 3
对称多项式 10
对称群 4,8,9,10
　多项式的～ 9
　多项式根的～ 10
　平面图形的～ 4
　数域 E 在 F 上的～ 8
多项式的分裂域 132

E

二次代数整数环 112
　实～ 112
　复～ 112
二次数环 110
二元运算 12

F

反同构 15,148
非平凡因式 106
非平凡因数 105
非平凡子群 19
分裂域 132
分式域 86

G

格 148
根式扩域 159
根闭理想 172
公倍式 106
公倍数 105
共轭 44,45
共轭元素类 44
共轭子群类 44
关系 33
轨道 68

H

函数环 74
合同关系 33
合同划分 33
恒等元 14
划分 33
环 73

Euclid～ 108
Gauss～ 111
I－进完备～ 87
Noether～ 173
p－进整数～ 88
多项式～ 94
函数～ 74
交换～ 73
商～ 80
一元多项式～ 95
一元多项式函数～ 95
整～ 84
子～ 76
环的表示 117
环的第二同态定理 82
环的第一同态定理 82
环的同构 78
环的同态 78
换位子 58

I

因式 106
因数 105
因子 107

J

基本域 126
奇置换 25
极大理想 101
极大条件 109
主理想满足～ 109
既约元 107
简约 Gröbner 基 184
交换环 73
交换群 3
交换自由半群 65
阶 18,122

K

可除代数 90
可解群 160

L

理想 79
极大～ 101
素～ 100
右～ 120
主～ 108
左～ 120
零因子 84
右～ 84
左～ 84
轮换 24

M

码 163
检错～ 163
纠错～ 164
线性～ 164
循环～ 168
码字 163
满同态 38,78
模 117
商～ 119
有限生成～ 122
周期～ 52,122
子～ 118
魔方群 30

N

内直和　47
内自同构　21
逆元　14

O

偶置换　25

P

偏序集　103
平面　1
平面图形的对称群　4
平移　2

Q

群　12
　Lie 型单～　54
　n 阶自由交换～　60
　n 元对称～　9
　变换～　13
　单～　53
　对称～　8,9
　交代～　55
　商～　35
　循环～　26
　有限～　13
　有限交换～　50
　域 F 上二阶射影特殊线性～　56
　真子～　19
　子～　19
　自同构～　6
　自由～　62
群代数　91
群的表示　121
群的第二同态定理　41
群的第一同态定理　40
群的作用　66

S

商环　80
商集　33
商模　119
商群　35
生成元集　20,77
数环　4
数域　5
数域 E 在 F 上的对称群　8
四元数　89
四元数代数　89
素理想　100
素域　100
素元　107
算术基本定理　105

T

特征　99
同构　14,69,119,133,148
　环的～　78
　模的～　119
　群的～　14
同态　38,78,119
　环的～　78
　模的～　119
　群的～　38
同态的核　38
同态象　38

W

外直和　50,119

外直积 50
微分算子环 77
唯一分解定理 106
唯一分解环 108
无限群 13

X

消去定理 189
形式 Lorentz 幂级数环 98
形式幂级数环 98
旋转 2
循环群 27
循环置换 24

Y

一一对应 1
一元多项式函数环 94
一元多项式环 94
因子 107
有限次扩域 126
有限单群 53
有限交换群 50
有限交换群结构定理 50
有限群 13
有限域 135
有序集 103
右 G－集 66
右 G－向量空间 121
右理想 120
右零因子 84
右陪集 36
余式 106
域 73
　代数闭～ 138
　单扩～ 130
　分裂～ 132
　分式～ 86
　扩～ 8
　有限～ 135
　有限次扩～ 126
　正规～ 138
　子～ 126
元素的阶 18
运动 1
运动群 3

Z

真理想 79
真因子 107
真子群 19
整除 107
整数环 74
整环 84
正规扩域 138
正规扩张 138
正规子群 21
指数 43
中间域 125
中心 18
中心元 20
主理想 107
主理想整环 108
子环 76
子模 118
子群 19,20
子域 126
自同构 5,21
　数域的～ 5
　群的～ 15
　域的～ 2

自同态 116
　加群的～ 116
自同态环 116
自由半群 64
自由群 62
最大公因式 106
最大公因数 105
最大似然译码原理 164
最大下界 148
最小公倍式 106
最小公倍数 105
最小上界 148
左 G-集 66
左理想 120
左零因子 84

An Introduction to Modern Algebra

ISBN 7-04-007450-8

9 787040 074505 >

定价 14.60 元